Broadview®
www.broadview.com.cn

“十一五”国家重点图书出版规划项目
国家信息安全等级保护系列丛书

信息安全
等级保护政策
培训教程

公安部信息安全等级保护评估中心　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全等级保护系列丛书

信息安全等级保护政策培训教程

公安部信息安全等级保护评估中心　编写

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本教程共 6 章，主要介绍开展信息安全等级保护工作的主要内容、信息安全等级保护政策体系和标准体系、信息系统定级与备案工作、信息安全等级保护安全建设整改工作、信息安全等级保护等级测评工作、安全自查和监督检查。

本教程对信息安全等级保护工作的有关政策、标准进行解读，对主要工作环节进行解释说明，可供有关部门在开展信息安全等级保护培训中使用。

图书在版编目（CIP）数据

信息安全等级保护政策培训教程 / 公安部信息安全等级保护评估中心编著. —北京：电子工业出版社，2010.6
（安全技术大系. 国家信息安全等级保护系列）
ISBN 978-7-121-10885-3

Ⅰ. ①信… Ⅱ. ①公… Ⅲ. ①信息系统－安全技术－技术培训－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2010）第 087929 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：许 艳
文字编辑：张丹阳
印 刷：北京智力达印刷有限公司
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：18.25 字数：248 千字
印 次：2010 年 6 月第 1 次印刷
印 数：4000 册 定价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国务院法规和中央文件明确规定，要实行信息安全等级保护，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。信息安全等级保护是当今发达国家保护关键信息基础设施、保障信息安全的通行做法，也是我国多年来信息安全工作经验的总结。开展信息安全等级保护工作不仅是保障重要信息系统安全的重大措施，也是一项事关国家安全、社会稳定、国家利益的重要任务。

近几年，为组织各单位、各部门开展信息安全等级保护工作，公安部根据法律授权，会同国家保密局、国家密码管理局和原国务院信息办组织开展了基础调查、等级保护试点、信息系统定级备案、安全建设整改等重要工作，出台了一系列政策文件，构成了信息安全等级保护政策体系，为指导各单位、各部门开展等级保护工作提供了政策保障。同时，在国内有关部门、专家、企业的共同努力下，公安部和标准化工作部门组织制订了信息安全等级保护工作的一系列标准，形成了信息安全等级保护标准体系，为开展信息安全等级保护工作提供了标准保障。

今后一段时期，公安机关、行业主管部门和信息系统运营使用单位将组织开展等级保护培训工作。我们结合近些年的工作实践，在公安部网络安全保卫局的指导下，编写了这本教程，对开展信息安全等级保护工作的主要内容、方法、流程、政策和标准等内容进行解读，对信息系统定级备案、安全建设整改、等级测评、安全检查等工作进行详细解释说明，供读者参考、借鉴。由于水平所限，书中难免有不足之处，敬请读者指正。

本书由公安部信息安全等级保护评估中心组织编写，在编写过程中得到国家网络与信息安全信息通报中心赵林副主任的大力支持和指导，在此表示由衷的感谢。参加编写的有周左鹰、郭启全、朱建平、毕马宁、景乾元、刘伟、范春玲、张秀东、祝国邦、马力、任卫红、李升、刘静等。

读者可以登录中国信息安全等级保护网 www.djbh.net，了解最新情况。

作　者

2010 年 5 月

目　　录

CHAPTER

1

第 1 章　信息安全等级保护制度的主要内容

本章主要介绍国家信息安全等级保护制度的有关法律、政策，信息安全等级保护工作的主要环节、流程和职责分工等，使读者对国家信息安全等级保护制度以及该制度如何实施有一个概括性的了解。

1.1　信息安全保障工作概述

1.1.1　加强信息安全工作的必要性和紧迫性

随着科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，信息化带动了工业化的发展，初步实现了互联互通、资源共享、跨越式发展的信息化发展目标。基础信息网络与重要信息系统的基础性、全局性作用日益增强，已成为国家和社会发展新的重要战略资源。与此同时，随着社会信息化的依赖程度越来越高，网络和信息系统的安全问题愈加重要。保障基础网络和重要信息系统安全，更好地维护国家安全、保障社会稳定和经济命脉，是信息化发展中必须要解决的重大问题。

但是，从总体上看，我国的信息安全保障工作尚处于初级阶段，基础薄弱，水平不高，存在许多亟待解决的问题。应当看到，我国信息安全面临的形势非常严峻，互联网上影响国家安全和社会稳定的问题日益突出，网上斗争越来越尖锐复杂。作为非传统安全范畴的信息安全问题，已经成为当前最难控制、最难把握的问题之一，国家必须高度重视信息安全，维护网络空间的国家安全和国家利益。

1.1.2 信息安全基本属性

信息安全是整体的、发展的、非传统的安全。信息安全涉及多个领域，是一个系统工程，需要全社会的共同努力和承担责任及义务；信息安全不是绝对的，它是动态的、相对的；信息安全不是一个国家能完全控制的问题，具有全球化特点，应从全球信息化角度考虑和布局；信息安全不是一个孤立的问题，应在系统建设过程中充分考虑；信息安全属于非传统安全问题，不能用传统的办法来解决非传统的安全问题，要有新的思路和手段。需要综合运用政策、法律、管理、技术等各种手段。

1.1.3 我国信息安全保障工作的确立

党中央、国务院高度重视信息安全保障工作。2003 年 7 月，国家信息化领导小组第三次会议专门研究信息安全问题，审议通过《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发［2003］27 号），首次明确了今后一段时期我国信息安全保障工作的总体要求、主要原则和重点任务，对加强信息安全保障工作做出了重要部署，要求建立国家信息安全保障体系。27 号文件将等级保护制度作为我国信息安全领域的一项基本制度予以明确，同时还提出了需要加强的信息保护和网络信任体系建设、信息安全监控体系建设、信息安全应急处理、信息安全技术研究开发、产业发展、法制和标准化建设、人才培养等一系列工作。2005 年 5 月，国家信

息化领导小组发布了《国家信息安全战略报告》（国信［2005］2 号），确定了今后一段时期国家信息安全的战略布局和长远规划。近期，国家还将出台新时期加强信息安全保障工作的意见，以进一步指导各地区、各部门开展信息安全工作。

1.1.4 信息安全保障工作的主要内容

我国信息安全保障工作要求坚持“积极防御、综合防范”的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。信息安全保障体系的主要内容包括：信息安全等级保护制度；加强以密码技术为基础的信息保护和网络信任体系建设；建设和完善信息安全监控体系；重视信息安全应急处理工作；加强信息安全技术研究开发，推进信息安全产业发展；加强信息安全法制建设和标准化建设；加快信息安全人才培养，增强全民信息安全意识；保证信息安全资金到位；加强对信息安全工作的领导，建立健全信息安全责任制。

1.1.5 保障信息安全的主要措施

保障信息安全的主要措施包括：一是建立完善的信息安全等级保护制度，加快信息安全工作的制度化；二是建立健全信息安全法律法规体系，推进信息安全法制建设；三是建立完善的信息安全标准体系，加强信息安全标准化工作；四是建立信息技术和信息安全技术体系，实现国家信息化发展的自主可控；五是完善信息安全监管体系，实现全方位的有效监管；六是完善信息安全监控体系，净化网络环境、维护网络秩序；七是建立健全信息网络违法犯罪防范打击体系，提高对信息网络违法犯罪的防范、控制、侦查、打击的能力；八是建立完善的信息安全通报和应急处置体系，为社会提供信息安全保障和服务；九是建立全社会的网络信任体系，保护国家利益、社会公共利益以及公民、法人和其他组织的合法权益；十是建立信息安全学科体系，加快信息安全人才的培养。

1.1.6 北京奥运会网络安全保卫成功经验给信息安全工作带来的启示

信息网络安全是北京“平安奥运”的重要组成部分，是北京奥运会成功举办的关键环节。由于赛前公安部组织协调有关部门和各方社会力量，综合采取了安全防护、监测预警、防范控制、应急准备等各项保障措施，从而确保了奥运会举办期间的信息网络安全。所有涉奥信息网络经受了大流量访问、网络入侵攻击等各种考验，没有发生一起网络中断、系统瘫痪的重大网络安全事件，确保了奥运会的顺利进行。为了确保涉奥信息网络完全，采取了如下主要措施。

1．建立跨部门的指挥协调机制

2007 年 9 月，经奥运安保工作协调小组批准，公安部牵头，会同 14 家单位专门组建了“信息网络安全指挥部”，建立了跨部门的指挥协调机制，统一指挥，加强协调，确立了指挥部工作会议制度、联络员工作会议制度、情况会商研判制度等协调联系机制，确保了奥运信息网络安保工作的顺利进行。经验证明，建立多部门的协调配合机制是应对重大活动时期信息网络安全的有效保障。

2．严格落实安全责任制

按照“谁主管谁负责、谁运营谁负责”的原则，根据《奥运信息网络安全保卫工作实施方案》以及赛时《奥运会信息网络安保勤务等级管理办法》和《奥运会信息网络安保工作指挥运行机制》要求，将奥运会 4 个核心网络和 31 个为奥运提供保障服务的网络信息系统作为重点保障对象，明确了公安部、奥组委、工信部、广电总、国务院新闻办、铁道部、人民银行、海关总署、民航总局、电监会、北京市公安局等部门对涉奥重要信息系统的安全责任，并组织督导检查，确保各项防范措施责任到人、落实到位。经验证明，落实信息安全责任制是保护重要信息系统安全的有效办法。

3．开展以信息安全等级保护为核心的安全防范工作

以奥运官方网站、竞赛网、票务系统、奥组委内外办公网等奥运会核心网络以

及 31 个为奥运提供保障服务的重要信息系统为重点，严格落实国家信息安全等级保护制度，组织开展了信息系统定级、备案、安全测评和渗透性攻击测试、风险评估，及时发现漏洞、安全隐患和问题，督促有关部门进行整改，提高了涉奥信息网络的安全防护能力。经验证明，落实等级保护制度，开展风险评估等工作是提高重要信息系统安全防范能力、抵御攻击能力的有效措施。

4．开展实时监测，及时预警

为提高对网络安全突发事件的发现和预警能力，公安部协调有关部门在赛前建立了多层多级的网络安全监测体系，对重要信息系统实行 24 小时实时监测，能够保证第一时间发现、预警网络异常、网络攻击和各类安全事件。经验证明，开展实时监测是保障重要信息系统运行安全的有效方法。

5．制定应急处置预案，加强演练

为确保突发网络安全事件时的应急处置及恢复，有关部门都制定了专门的应急预案，并按照预案进行演练，磨合了应急指挥协调机制和工作流程，储备了应急资源和防护手段，做好了各项应急恢复准备，从而确保了一旦突发网络安全事件，能够在第一时间反应、果断妥善处置。经验证明，制定预案并加强演练是提高处置重要信息系统突发安全事件有效方法。

1.2 信息安全等级保护的基本含义

1.2.1 信息安全等级保护的法律和政策依据

1．法律依据

1994 年《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号）第九条明确规定：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。该条明确了三个内容：一是确

立了等级保护是计算机信息系统安全保护的一项制度；二是出台配套的规章和技术标准；三是明确了公安部在等级保护工作中在等级保护工作中的牵头地位。

2．政策依据

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出：“实行信息安全等级保护。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。标志着等级保护从计算机信息系统安全保护的一项制度提升到国家信息安全保障工作的基本制度。同时中央 27 号文明确了各级党委和政府在信息安全保障工作中的领导地位，以及“谁主管谁负责，谁运营谁负责”的信息安全保障责任制。

1.2.2　什么是信息安全等级保护

1．基本概念

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

信息系统是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

2．信息安全等级保护工作的内涵

简单来说，信息安全等级保护就是分等级保护、分等级监管，是将全国的信息系统（包括网络）按照重要性和遭受损坏后的危害性分成五个安全保护等级（从第一级到第五级，逐级增高）；等级确定后，第二级（含）以上信息系统到公安机关备

案，公安机关对备案材料和定级准确性进行审核，审核合格后颁发备案证明；备案单位根据信息系统安全等级，按照国家标准开展安全建设整改，建设安全设施、落实安全措施、落实安全责任、建立和落实安全管理制度；备案单位选择符合国家规定条件的测评机构开展等级测评；公安机关对第二级信息系统进行指导，对第三、四级信息系统定期开展监督、检查。

根据《信息安全等级保护管理办法》的规定，等级保护工作主要分为五个环节，定级、备案、建设整改、等级测评和监督检查。其中定级是信息安全等级保护的首要环节，通过定级，可以梳理各行业、各部门、各单位的信息系统类型、重要程度和数量等，确定信息安全保护的重点。而安全建设整改是落实信息安全等级保护工作的关键，通过建设整改使具有不同等级的信息系统达到相应等级的基本保护能力，从而提高我国基础网络和重要信息系统整体防护能力。等级测评工作的主体是第三方测评机构，通过开展等级测评，可以检验和评价信息系统安全建设整改工作的成效，判断安全保护能力是否达到相关标准要求。监督检查工作的主体是公安机关等信息安全职能部门，通过开展监督、检查和指导，维护重要信息系统安全和国家安全。

3．信息安全等级保护是基本制度、基本国策

信息安全等级保护是党中央国务院决定在信息安全领域实施的基本国策，由公安部牵头经过近十年的探索和实践，信息安全等级保护的政策、标准体系已经基本形成，已在全国范围内全面开展实施。

信息安全等级保护制度是国家信息安全保障工作的基本制度，是落实网络信任体系、安全监控体系、应急处理、风险评估、灾难备份、技术开发和产业发展等信息安全保障工作的基础。开展信息安全等级保护工作是实现国家对重要信息系统重点保护的重大措施。信息安全等级保护制度的核心内容是，国家制定统一的政策，各单位、各部门依法开展等级保护工作，有关职能部门对信息安全等级保护工作实施监督管理。

4．信息安全等级保护是基本方法

信息安全等级保护也是国家信息安全保障工作的基本方法。等级保护制度提出了一整套安全要求，贯穿系统设计、开发、实现、运维、废弃等系统工程的整个生命周期，引入了测评技术、风险评估、灾难备份、应急处置等技术。按照等级保护制度中规定的五个动作“定级、备案、建设、测评、检查”，各单位各部门开展信息安全工作，先对所属信息系统（包括信息网络）开展调查摸底、梳理信息系统，再对信息系统定级，定级后二级以上系统到公安机关备案，然后按标准进行安全建设整改，开展等级测评。公安机关按照系统级别实施不同强度的监管，对进入重要信息系统的测评机构以及信息安全产品分等级进行管理，对信息安全事件分等级响应和处置。经过一系列工作的开展，将信息安全保障工作落到了实处。

1.2.3　公安机关组织开展等级保护工作的法律、政策依据

（1）《中华人民共和国警察法》。《中华人民共和国警察法》第六条第十二款规定，公安机关人民警察依法履行“监督管理计算机信息系统的安全保护工作”。组织开展信息安全等级保护工作是公安机关在信息网络领域开展的面向全社会的管理监察工作，是公安机关在社会信息化条件的一项新的职责。实施信息安全等级保护是公安机关依法保障重要信息系统安全的重要手段。

（2）《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号）。本条例第六条规定：“公安部主管全国计算机信息系统安全保护工作”，第九条规定：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

（3）2008 年国务院三定方案明确规定公安机关在信息安全等级保护工作中的职能：监督、检查、指导信息安全等级保护工作。

（4）2004 年 7 月 3 日国家网络与信息安全协调小组第三次会议审议通过了《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号），进一步明确公安机关负

责全国信息安全等级保护工作的监督、检查和指导工作，并指出“要建立专门的等级保护监督检查机构和技术支撑体系，组织研制、开发科学、实用的检查、评估工具，充实力量，加强建设，切实承担信息安全等级保护监督、检查和指导的职责。”

（5）2007 年公安部、国家保密局、国家密码管理局等四部门联合出台的《信息安全等级保护管理办法》（公通字[2006]43 号）详细阐述了公安机关的具体工作任务。公安部牵头，会同国家保密局、国家密码管理局等部门共同组织全国各单位、各部门实施信息安全等级保护工作。同时，公安机关还承担信息安全等级保护监督、检查、指导的任务。这是党中央、国务院交给公安机关的新任务，在信息化时代公安机关巩固党的执政地位、维护国家长治久安、保障人民安居乐业的新职责。

1.2.4 贯彻落实信息安全等级保护制度的原则

国家信息安全等级保护坚持自主定级、自主保护的原则，对信息系统分等级进行保护，按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则。

（1）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

（2）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

（3）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（4）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。

国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括：国家事务处理信息系统（党政机关办公系统）；财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统；教育、国家科研等单位的信息系统；公用通信、广播电视传输等基础信息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其他领域的重要信息系统。

1.2.5 信息系统安全保护等级的划分与监管

1．五个安全保护等级划分

信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。信息系统的安全保护等级共分五级。

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

2．五级保护与监管

信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

3．信息安全产品管理和信息安全事件实行分等级响应、处置的制度

国家对信息安全产品的使用实行分等级管理。

信息安全事件实行分等级响应、处置的制度。依据信息安全事件对信息和信息系统的破坏程度、所造成的社会影响以及涉及的范围，确定事件等级。根据不同安全保护等级的信息系统中发生的不同等级事件制定相应的预案，确定事件响应和处置的范围、程度以及适用的管理制度等。信息安全事件发生后，分等级按照预案响应和处置。

1.3 实行信息安全等级保护制度的必要性和紧迫性

1.3.1 为什么要强制实行信息安全等级保护制度

建立和落实信息安全等级保护制度是形势所迫、国情所需。随着我国信息化进

程的全面加快，全社会特别是重要行业、重要领域对基础信息网络和重要信息系统的依赖程度越来越高，基础信息网络和重要信息系统业已成为国家关键基础设施，其安全性直接关系到国家安全、国家利益、社会稳定和人民群众的切身利益。但是，我国基础信息网络和重要信息系统安全面临的形势十分严峻。

1．强制实施等级保护制度是信息安全形势所迫

一是来自境内外敌对势力的入侵、攻击、破坏越来越严重。境内外各种势力、组织和别有用心的人利用各种手段利用信息网络或针对信息网络实施各种破坏活动。境外敌对势力和情报机构通过木马入侵、远程控制我重要信息系统计算机的案件，大量窃取国家秘密的事件不断发生。基础信息网络和重要信息系统日益成为境外敌对势力和间谍情报机构攻击窃密的重点目标。

二是针对基础信息网络和重要信息系统的违法犯罪持续上升。不法分子利用一些安全漏洞，使用病毒、木马、网络钓鱼等技术进行网络盗窃、网络诈骗、黑客攻击等违法犯罪活动，对我国的经济秩序、社会管理秩序和公民的合法权益造成严重侵害。网络攻击仍是当前网络安全的主要威胁。网站成为主要攻击目标，利用网站“挂马”现象日趋严重。据监测，2008 年大陆地区共有 58.5 万多个 IP 地址对应的主机被来自境外的木马秘密控制，利用木马和“僵尸网络”实施分布式拒绝服务攻击的威胁加剧，防范难度越来越大。安全漏洞数量居高不下。据统计，2008 年共发现 4103 个系统安全漏洞，其中高危漏洞占近一半。2008 年新发现的系统安全漏洞中有一半以上没有安全补丁，及时修补安全漏洞是导致安全事件发生的最主要原因。针对“零日”漏洞出现的攻击不断增加，利用国产应用软件漏洞进行网络攻击成为新的发展趋势。病毒传播感染情况严重。2008 年新增病毒 46 万余种，较 2007 年上升 5.6%，感染计算机 3.62 亿台次，较 2007 年上升 86.4%，新增病毒中木马类病毒占 60%。病毒制作、传播、销售的组织化、产业化、互联网化特征日趋明显，大量木马、后门病毒通过“网站挂马”、伪造和欺骗等手段传播蔓延，消耗系统资源，危害网络系统的安全运行。

2．强制实施等级保护制度是国情所需

一是基础信息网络和重要信息系统安全隐患严重。由于各基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口，短时期无法实现自主可控，给我国的信息安全带来了深层的安全隐患。信息安全建设与信息化建设不同步，建设不规范、不全面。据备案数据统计，我国基础信息网络和重要信息系统的多数核心软、硬件设备（服务器、存储设备、操作系统等）和高端服务仍严重依赖于国外，国外产品的采用率高达 80%以上，相当一部分信息系统由国外公司提供技术服务。大量重要信息系统存在不同程度的安全漏洞和隐患。采购中忽视了维护我方信息安全利益的具体要求和对信息安全风险控制措施，相应的安全管理和控制措施又明显不足，存在外部威胁源入侵控制的隐患。现有的信息安全产品管理理念和模式不适应形势的发展，以信息技术产品安全性、可控性管理为主要内容的产品管理模式亟待建立。

二是我国的信息安全保障工作基础还很薄弱。我国信息安全建设与信息化建设不同步，信息安全工作缺乏国家层面的制度化规定和有效监管，信息系统安全建设、监管缺乏标准规范，许多部门安全管理制度和技术防范措施不落实等。因入侵攻击、设备故障、人为破坏以及保障系统等因素导致的网络安全事件时有发生。一些重要信息系统多次发生因设备问题导致系统出现运行故障的事件。安全防范技术措施落实不到位。突出表现在移动存储介质管理与使用不善，造成木马病毒传播、数据丢失和失密泄密；内网系统安全补丁更新不及时；内外网安全隔离措施不完备，网络访问控制不严密；未关闭不必要的端口和服务，为网络入侵提供了可乘之机；安全保密意识薄弱、保密措施落实不到位、安全管理存在漏洞，被境外间谍情报机构入侵窃密的情况时有发生。风险抵御能力不强，主要是网络基础设施建设中安全系统建设相对滞后，重建设轻维护现象依然存在；随着数据集中、系统整合的逐步推进，数据存储、传输、应用等方面的安全风险相应增大；运行维护经费保障与人员力量严重不足；应急设施不完备，应急演练不充分，有效应对重大自然灾害和大规模、有预谋、有组织网络攻击的能力有待提高。

可以预见，我国基础信息网络和重要信息系统如果发生信息网络安全故障，将

严重影响其保障服务的顺利进行；如果遭遇网络入侵，将导致有关国家秘密文件或敏感信息被窃取、重要数据被篡改、系统不能正常运行；如果受到网站攻击，将致使政府门户网站和重点新闻网站访问被中断、页面被篡改，甚至系统瘫痪，对我国国家安全、社会秩序、公共利益等造成严重影响。因此，实施信息安全等级保护，将信息系统根据其重要程度进行分级，突出保护的重点，已成为各级领导、各部门以及全社会的共识。国内外形势和国情现状决定了我国必须尽快建立一个适合国情的信息安全制度，突出重点，保护重点，统筹监管，保障信息安全，维护国家安全。

面对信息安全面临的复杂、严峻的形势，基础信息网络和重要信息系统一旦出现大的信息安全问题，不仅仅影响本单位、本行业，而是直接威胁国家安全、社会稳定、经济发展。胡锦涛总书记等中央领导同志对信息安全工作始终给予高度重视，先后多次做出重要指示。胡锦涛总书记明确指出，当前，国际上围绕信息获取、利用、控制的斗争日趋激烈，维护国家在网络空间的安全和利益成为信息时代的重大战略课题。要求我们必须敏锐地把握当今世界信息化发展的趋势，积极推进国民经济和社会信息化，确保我国在日趋激烈的国际竞争中掌握主动权。

1.3.2 实施信息安全等级保护制度能解决什么问题

通过开展信息安全等级保护工作，可以充分体现“明确重点、突出重点、保护重点”的目的，将有限的财力、物力、人力投入到重要信息系统安全保护中，按标准建设安全保护措施，建立安全保护制度，落实安全责任，有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统的安全，有效提高我国信息安全保障工作的整体水平，有效解决我国信息安全面临的威胁和存在的主要问题。

信息安全等级保护是当今发达国家保护关键信息基础设施、保障信息安全的通行做法，也是我国多年来信息安全工作经验的总结。实施信息安全等级保护，有利于在信息化建设过程中同步建设信息安全设施，将信息安全保障与信息化建设相协调；有利于为信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务；

有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。几年来的实践证明，等级保护工作是各单位、各部门开展信息安全保障工作的抓手，也是信息安全保障工作的灵魂。

1.3.3 国外实施等级保护的经验和做法

信息安全分级保护是当今发达国家保护关键信息基础设施，保障信息安全的通行做法。国外多是以分级为手段，以保护国家关键基础设施为目的，从落实监管部门、制定政策和标准、实施安全建设等方面提高对涉及国家安全的关键基础设施实施整体安全防护。

1．明确专门部门负责监管

2004 年 1 月，美国成立了“全国信息保障委员会”、“全国信息保障同盟”和“关键基础设施信息保障办公室”等 10 多个全国性信息安全机构。911 事件后，美国将信息安全监管的职责交给了新成立的国土安全部。布什总统将克林顿成立的“总统关键基础设施保护委员会”这一部委之间的协调机构改为行政实体“总统关键基础设施保护办公室”，接受总统办公厅直接领导。美国联邦政府其他部门在维护信息安全的职责是：商务部发布有关计算机安全的标准和指导方针；国防部属下的国家安全局主要负责保密信息系统（被有关法规称为“国家安全系统”）的信息安全工作；计算机应急处理小组协调中心负责提供 24 小时可靠、可信的紧急情况联络，促进专家之间的交流以便解决信息安全问题等。

奥巴马执政以来，美国高度重视网络安全问题，将网络空间视为继陆、海、空、太空后的“第五战略空间”，制订出台了包括强化联邦政府对网络安全的统一领导，整合各方资源力量，成立作战部队，加强技术研发和网络战资源储备等一系列重要

举措，全面提升国家关键信息基础设施的安全防范能力。2009 年奥巴马政府在国家安全参谋部内设立“网络安全办公室”作为国家网络安全事务的最高协调指挥机构，设立一名网络安全协调员（Cyber tsar，又称“网络沙皇”），作为国家安全委员会和国家经济委员会的成员，以解决原来根据“国家网络安全综合计划”（CNCI）设立的“国家网络安全中心”对网络安全事务协调不力的问题。

2．制定信息安全防护政策

1998 年 5 月美国总统克林顿签发了第 63 号总统令，提出了信息保障的概念，第一次就美国信息安全的概念、意义、长期与短期目标等作了明确的说明，并针对下一步的行动做了指示。据此，1998 年 1 月国防部制定了《国防信息保障纲要》，1998 年 5 月又制定了《信息保障技术框架》。2002 年，美国通过的《联邦信息安全管理法案》规定必须对联邦政府信息系统进行安全评估并备案，为美国政府机构信息系统改善信息安全问题设定了目标，也被称做美国电子政务法案。

3．制定技术标准

以《可信计算机系统评估准则》为核心的彩虹系列标准代表着美国以计算机分级为手段保护关键基础设施的思路。《信息保障技术框架（IATF）》、《联邦信息处理标准（NIST）》等一系列标准，确定了以分等级保护、重点保护国家关键信息基础设施为核心的国家信息安全保障体系。其中 IATF 提出了“多点防护、分层防御”的概念，指出当确信信息与信息系统已通过可用性、完整性、鉴别、保密性、不可否认性等安全服务而受到保护时，便实现了 IA（信息保障）。

4．实施信息安全工程建设

美国政府 2003 年财政预算有 7.22 亿美元用于信息安全建设，以防止遭受恐怖袭击。其中引人注目的是“政府专用网”（GOVNET）研究计划，建立一个连接联邦机构的保密网络，采用合适的技术与因特网隔离。美国政府认为，如果政府在互联网安全方面不投入更多的资金，那么“数字珍珠港”事件总有一天会爆发。恐怖分子

完全可能破坏美国的信息基础设施，控制电信、电网、水力供应和空中交通的计算机网络。

1.4 信息安全等级保护制度的主要内容

1.4.1 等级保护工作中有关部门的责任和义务

国家、有关部门和企业在信息安全等级保护工作中有着不同的责任和义务。

1．国家层面

通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

2．信息安全监管部门

信息安全监管部门包括公安机关、保密部门、国家密码工作部门。组织制定等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统实行分等级安全保护，对等级保护工作的实施进行监督、管理。

公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。

在信息安全等级保护工作中，坚持“分工负责、密切配合”的原则。公安机关牵头，负责全面工作的监督、检查、指导，国家保密工作部门、国家密码管理部门配合。因为涉及国家秘密信息系统中也会发生信息安全问题和密码问题，所以，涉及国家秘密的信息系统，主要由国家保密工作部门负责，其他部门参与、配合，因为非涉及国家秘密的信息系统中也会发生保密问题和密码问题，所以，

非涉及国家秘密的信息系统，主要由公安机关负责，其他部门参与、配合。需要强调的是，涉及工作秘密、商业秘密的信息系统不属于涉密信息系统。

3．信息系统主管部门

依照《信息安全等级保护管理办法》及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

4．信息系统运营使用单位

按照国家有关等级保护的管理规范和技术标准开展等级保护工作，建设安全设施、建立安全制度、落实安全责任，接受公安机关、保密部门、国家密码工作部门对信息安全等级保护工作的监督、指导，保障信息系统安全。

5．安全服务机构

信息安全企业，信息系统安全集成商、等级测评机构等安全服务机构，依据国家有关管理规定和技术标准，开展技术支持、服务等工作，并接受监管部门的监督管理。

1.4.2　等级保护工作的主要环节和基本要求

1．等级保护的主要环节

等级保护的主要环节：定级、备案、安全建设整改、等级测评和安全检查。

一是信息系统定级。信息系统定级按照自主定级、专家评审、主管部分审批、公安机关审核的流程进行。信息系统运营使用单位按照《信息安全等级保护管理办法》（公通字[2007]43 号，以下简称《管理办法》）和《信息系统安全等级保护定级指南》（GB/T22240-2008），自主确定信息系统的安全保护等级。为保证信息系统定级准确，可以组织专家进行评审。有上级主管部门的，应当经上级主管部门审批，跨省或全国统一联网运行的信息系统可以由其主管部门统一确定安全保护等级。最后，

经公安机关审核把关，合理确定信息系统安全保护等级。

二是信息系统备案。第二级以上信息系统，由信息系统运营使用单位到所在地设区的市级以上公安机关网络安全保卫部门办理备案手续。公安机关按照《信息安全等级保护备案实施细则》（公信安[2007]1360 号）要求，对备案材料进行审核，定级准确、材料符合要求的颁发由公安部统一监制的备案证明。

三是信息系统安全建设整改。信息系统安全保护等级确定后，运营使用单位按照《管理办法》、《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）等有关管理规范和技术标准，选择《管理办法》要求的信息安全产品，制定并落实安全管理制度。落实安全责任，建设安全设施，落实安全技术措施。

四是等级测评。信息系统建设整改完成后，运营使用单位选择符合要求的测评机构，依据《管理办法》和《信息系统安全等级保护测评要求》和《信息系统安全等级保护测评过程指南》标准，对信息系统安全保护状况开展等级测评，按照《信息系统安全等级测评报告模版（试行）》（公信安[2009]1487 号）编写等级测评报告。

五是监督检查。公安机关依据《管理办法》和《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736 号），监督检查运营使用单位开展等级保护工作，定期对第三级以上的信息系统进行安全检查。运营使用单位应当接受公安机关的安全监督、检查、指导，如实向公安机关提供有关材料。

2．开展等级保护工作的基本要求

各基础信息网络和重要信息系统，按照（“准确定级、严格审批、及时备案、认真整改、科学测评”）的要求完成等级保护的定级、备案、整改、测评等工作。公安机关和保密、密码工作部门要及时开展监督检查，严格审查信息系统所定级别，严格检查信息系统开展备案、整改、测评等工作。对故意将信息系统安全级别定低，逃避公安、保密、密码部门监管，造成信息系统出现重大安全事故的，要追究单位和相关人员的责任。

1.5 实施等级保护制度的工作情况

近几年，公安部以及省、市公安机关按照法律、政策规定，按照党中央、国务院的部署，组织开展了大量工作，为全面实施等级保护制度奠定了坚实基础。

1.5.1 基础调查

2005 年底，公安部会同有关部门联合印发了《关于开展信息系统安全等级保护基础调查工作的通知》，于 2006 年上半年在全国范围内开展了信息系统安全等级保护基础调查。调查了 6 万多家单位，11 万个信息系统。通过基础调查，基本摸清和掌握了全国信息系统特别是重要信息系统的基本情况，为制定信息安全等级保护政策、部署全国开展等级保护工作奠定了坚实的基础。

1.5.2 等级保护试点工作

为探索方法，验证思路，2006 年 6 月，公安部、国家保密局、国家密码管理局等四部门下发了《关于开展信息安全等级保护试点工作的通知》，在 13 个省区市和 3 个部委开展了信息安全等级保护试点工作。通过试点，完善了开展等级保护工作的模式和思路，检验和完善了开展等级保护工作的方法、思路、规范标准，探索了开展等级保护工作领导、组织、协调的模式和办法，为全面开展等级保护工作奠定了坚实的基础。

1.5.3 部署定级备案工作

2007 年 7 月，公安部等四部门联合发布了《关于开展全国重要信息系统安全等级保护定级工作的通知》，在北京联合召开了“全国重要信息系统安全等级保护定级工作电视电话会议”，国家信息安全职能部门、基础信息网络和重要信息系统主管部

门、各省（区、市）公安厅（局）、保密局、国家密码管理局、信息化领导小组办公室和有关行业、部门的负责同志出席了会议，部署在全国范围内开展重要信息系统安全等级保护定级工作，标志着国家信息安全等级保护制度在全国开始全面实施。

全国重要信息系统等级保护定级工作完成后，公安部向周永康、刘云山、曾培炎同志做了专报《关于全国重要信息系统安全等级保护定级工作情况的报告》（公部[2008]11 号），得到中央领导批示。

1.5.4 等级测评体系建设试点工作

为探索信息安全等级保护测评体系建设和管理的模式和经验，保障全国重要信息系统等级保护安全建设工作顺利开展，公安部于 2009 年 7 月至 10 月组织开展了信息安全等级保护测评机构体系建设试点工作。

1．试点组织情况

试点工作由公安部网络安全保卫局统一领导，浙江、河南、重庆、广东省公安厅、局公共信息网络安全监察总队以及宁波、深圳市公安局公共信息网络安全监察支队、国家电力监管委员会信息中心具体组织实施，公安部信息安全等级保护评估中心、北京网络行业协会信息系统测评中心、工业和信息化部计算机安全技术检测中心负责试点的技术支持工作。

2．试点目的

（1）探索建立地区性、行业性信息安全等级测评机构的模式及测评机构能力建设和确认的内容和方法，完善测评机构规范化建设要求；探索测评人员条件、能力以及资格等内容和要求，为在各地区和重点行业建立等级测评机构提供经验。

（2）探索部级测评机构在推进地区性和行业性测评机构建设中承担的职责任务及其应具备的能力、资质，为发挥部级测评机构在测评体系建设中的作用提供经验。

（3）探索测评机构等级测评活动的规范化要求的内容和方法，检验并完善等级

测评报告格式及有关测评标准，为提高等级测评工作水平提供经验。

（4）探索对测评机构监督管理的内容和方法，检验并完善等级测评机构有关的技术标准和《信息安全等级保护等级测评机构和测评人员管理细则》等管理规范，为测评机构规范化、标准化建设和管理提供依据。

3．试点成效

此次试点工作是等级测评体系建设的一次全面实践和检验，主要工作成效：一是检验了等级测评机构条件的必要性和可行性。二是探索了行业性、地区性信息安全等级测评机构组建模式。三是检验并完善了等级测评活动规范化要求的科学性、适用性。四是检验并完善了测评师培训和测评机构能力评估流程和方法。五是检验并完善了的规范、标准。六是锻炼了队伍，提高了测评业务能力和水平。

1.5.5 等级保护协调（领导）机构和专家组建设

1．等级保护协调（领导）机构建设

为加强信息安全等级保护工作的领导，公安部、国家保密局、国家密码管理局联合成立了由公安部张新枫副部长任组长的国家信息安全等级保护工作协调小组，办公室设在公安部网络安全保卫局。各省、地市也成立了信息安全等级保护工作协调（领导）小组，办公室设在公安厅（局）网络警察总（支）队。

2．等级保护专家组建设

为了充分调动和发挥信息安全专家的作用，为重要行业、重要部门开展等级保护安全建设整改工作提供技术支持和指导，有效服务于信息安全等级保护工作，国家成立了信息安全等级保护安全建设指导委员会（名单见附录K），各省（区、市）均成立了信息安全等级保护专家组。专家组的主要职责是：

（1）配合公安部宣传信息安全等级保护安全建设相关政策，根据等级保护安全建设总体部署，指导备案单位研究拟定信息安全等级保护安全建设的贯彻实施意见

和建设规划；

（2）宣传国家信息安全等级保护安全建设相关技术标准，并结合行业特点，研究、指导备案单位等级保护安全建设相关技术标准的行业应用，指导备案单位研究拟定行业技术标准规范；

（3）参与备案单位信息安全等级保护安全建设整改方案的论证、评审，指导备案单位信息安全等级保护安全建设工作；

（4）了解掌握并研究探索行业开展信息安全等级保护安全建设工作中安全管理、安全技术和工程建设、工程管理等最佳实践，总结成功经验，树立典型并提出推广意见；

（5）跟踪国内外信息安全技术最新发展，组织和引导信息安全研究机构和企业开展信息安全等级保护共性技术和关键技术专题研究，推动等级保护技术研究工作，促进信息安全产业发展；

（6）研究提出完善国家信息安全等级保护政策体系和技术体系的意见和建议。

CHAPTER

2

第 2 章　信息安全等级保护政策体系和标准体系

本章系统介绍了信息安全等级保护的有关政策和标准，并对有关政策文件和标准的应用进行了简要说明。

2.1　信息安全等级保护政策体系

近几年，为组织开展信息安全等级保护工作，公安部根据《中华人民共和国计算机信息系统安全保护条例》的授权，会同国家保密局、国家密码管理局、原国务院信息办和发改委出台了一些文件，公安部对有些具体工作出台了一些指导意见和规范，这些文件初步构成了信息安全等级保护政策体系（如图 2-1 所示），为指导各地区、各部门开展等级保护工作提供了政策保障。

为了方便读者使用，本书将信息安全等级保护有关政策文件列为附录内容。

2.1.1　总体方面的政策文件

总体方面的文件有两个，这两个文件确定了等级保护制度的总体内容和要求，对等级保护工作的开展起到宏观指导作用。

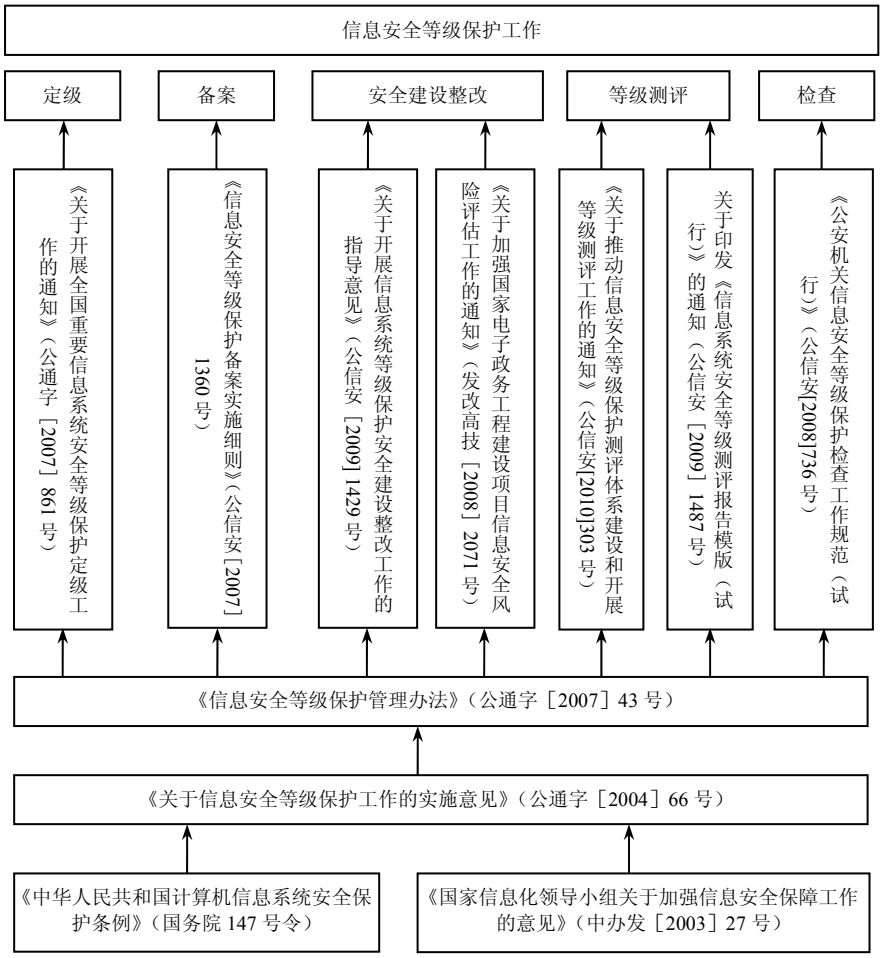

图 2-1　信息安全等级保护法律政策体系

1.《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

该文件是为贯彻落实国务院第 147 号令和中办 27 号文件，由公安部、国家保密局、国家密码管理局、原国务院信息办等四部委共同会签印发，指导相关部门实施信息安全等级保护工作的纲领性文件，主要内容包括贯彻落实信息安全等级保护制度的基本原则，等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责分工等。

2.《信息安全等级保护管理办法》（公通字[2007]43 号）

该文件是在开展信息系统安全等级保护基础调查工作和信息安全等级保护试点工作的基础上，由四部委共同会签印发的重要管理规范，主要内容包括信息安全等级保护制度的基本内容、流程及工作要求，信息系统定级、备案、安全建设整改、等级测评的实施与管理，信息安全产品和测评机构选择等。该文件为开展信息安全等级保护工作提供了规范保障。

2.1.2 具体环节的政策文件

对应等级保护工作的具体环节（信息系统定级、备案、安全建设整改、等级测评、安全检查），公安部出台了相应的政策规范。

1．定级环节

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字[2007]861 号，以下简称《定级工作通知》）。2007 年 7 月 20 日四部委在北京联合召开了“全国重要信息系统安全等级保护定级工作电视电话会议”，会议根据该通知精神部署在全国范围内开展重要信息系统安全等级保护定级工作，标志着全国信息安全等级保护工作全面开展。该文件由四部委共同会签印发。

2．备案环节

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）。该文件规定了公安机关受理信息系统运营使用单位信息系统备案工作的内容、流程、审核等内容，并附带有关法律文书，指导各级公安机关受理信息系统备案工作。该文件由公安部网络安全保卫局印发。

3．安全建设整改环节

（1）《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429

号）。该文件明确了非涉及国家秘密信息系统开展安全建设整改工作的目标、内容、流程和要求等，文件附件包括《信息安全等级保护安全建设整改工作指南》和《信息安全等级保护主要标准简要说明》。该文件由公安部印发。

（2）《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）。该文件要求非涉密国家电子政务项目开展等级测评和信息安全风险评估要按照《信息安全等级保护管理办法》进行，明确了项目验收条件：公安机关颁发的信息系统安全等级保护备案证明、等级测评报告和风险评估报告。该文件由发改委、公安部、国家保密局共同会签印发。

4．等级测评环节

（1）《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）。为了规范等级测评活动，加强对侧评机构及测评人员的管理，在等级侧评体系建设试点工作的基础上，公安部网络安全保卫局出台了该文件。该文件确定了开展信息安全等级保护测评体系建设和等级测评工作的目标、内容、和工作要求。该文件附有《信息安全等级保护测评工作管理规范》，规定了测评机构的条件、业务范围和禁止行为，规范了测评机构的申请、受理、测评能力评估、审核、推荐的流程和要求，规范了等级测评师培训、考试、获证的流程和要求，规范了测评机构开展测评活动的内容和要求，规范了对测评机构的监督、检查和指导内容，确保测评机构的水平和能力符合要求以及测评活动客观、公正和安全。以利于等级侧评机构的规范化、制度化建设，为等级侧评工作的顺利开展提供政策支持。

（2）关于印发《信息系统安全等级测评报告模版（试行）》的通知（公信安[2009]1487 号）。该文件明确了等级测评活动的内容、方法和测评报告格式等内容，用以规范等级测评报告的主要内容。该文件由公安部网络安全保卫局印发。

5．安全检查环节

《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736 号）。该文件规定了公安机关开展信息安全等级保护检查工作的内容、程序、方式以及相关

法律文书等，使检查工作规范化、制度化。该文件由公安部网络安全保卫局印发。

2.2 信息安全等级保护标准体系

为推动我国信息安全等级保护工作，十多年来，在公安部的领导和支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制订了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系，为开展信息安全等级保护工作提供了标准保障。信息安全等级保护相关标准具体见《信息安全等级保护主要标准简要说明》。

2.2.1 信息安全等级保护相关标准类别

信息安全等级保护相关标准大致可以分为四类：基础类、应用类、产品类和其他类。

1．基础类标准

《计算机信息系统安全保护等级划分准则》（GB17859—1999）。

2．应用类标准

（1）信息系统定级

《信息系统安全保护等级定级指南》（GB/T 22240—2008）。

（2）等级保护实施

《信息系统安全等级保护实施指南》（信安字[2007]10 号）。

（3）信息系统安全建设

《信息系统安全等级保护基本要求》（GB/T 22239—2008）；

《信息系统通用安全技术要求》（GB/T 20271—2006）；

《信息系统等级保护安全设计技术要求》（GB/T24856—2009）；

《信息系统安全管理要求》（GB/T 20269—2006）；

《信息系统安全工程管理要求》（GB/T 20282—2006）；

《信息系统物理安全技术要求》（GB/T 21052—2007）；

《网络基础安全技术要求》（GB/T 20270—2006）；

《信息系统安全等级保护体系框架》（GA/T 708—2007）；

《信息系统安全等级保护基本模型》（GA/T 709—2007）；

《信息系统安全等级保护基本配置》（GA/T 710—2007）。

（4）等级测评

《信息系统安全等级保护测评要求》（报批稿）；

《信息系统安全等级保护测评过程指南》（报批稿）；

《信息系统安全管理测评》（GA/T 713—2007）。

3．产品类标准

（1）操作系统

《操作系统安全技术要求》（GB/T 20272—2006）；

《操作系统安全评估准则》（GB/T 20008—2005）。

（2）数据库

《数据库管理系统安全技术要求》（GB/T 20273—2006）；

《数据库管理系统安全评估准则》（GB/T 20009—2005）。

（3）网络

《网络端设备隔离部件技术要求》（GB/T 20279—2006）；

《网络端设备隔离部件测试评价方法》（GB/T 20277—2006）；

《网络脆弱性扫描产品技术要求》（GB/T 20278—2006）；

《网络脆弱性扫描产品测试评价方法》（GB/T 20280—2006）；

《网络交换机安全技术要求》（GA/T 684—2007）；

《虚拟专用网安全技术要求》（GA/T 686—2007）。

（4）PKI

《公钥基础设施安全技术要求》（GA/T 687—2007）；

《PKI 系统安全等级保护技术要求》（GB/T 21053—2007）。

（5）网关

《网关安全技术要求》（GA/T 681—2007）。

（6）服务器

《服务器安全技术要求》（GB/T 21028—2007）。

（7）入侵检测

《入侵检测系统技术要求和检测方法》（GB/T 20275—2006）；

《计算机网络入侵分级要求》（GA/T 700—2007）。

（8）防火墙

《防火墙安全技术要求》（GA/T 683—2007）；

《防火墙技术测评方法》（报批稿）；

《信息系统安全等级保护防火墙安全配置指南》（报批稿）；

《防火墙技术要求和测评方法》（GB/T 20281—2006）；

《包过滤防火墙评估准则》（GB/T 20010—2005）。

（9）路由器

《路由器安全技术要求》（GB/T 18018—2007）；

《路由器安全评估准则》（GB/T 20011—2005）；

《路由器安全测评要求》（GA/T 682—2007）。

（10）交换机

《网络交换机安全技术要求》（GB/T 21050—2007）；

《交换机安全测评要求》（GA/T 685—2007）。

（11）其他产品

《终端计算机系统安全等级技术要求》（GA/T 671—2006）；

《终端计算机系统测评方法》（GA/T 671—2006）；

《审计产品技术要求和测评方法》（GB/T 20945—2006）；

《虹膜特征识别技术要求》（GB/T 20979—2007）；

《虚拟专网安全技术要求》（GA/T 686—2007）；

《应用软件系统安全等级保护通用技术指南》（GA/T 711—2007）；

《应用软件系统安全等级保护通用测试指南》（GA/T 712—2007）；

《网络和终端设备隔离部件测试评价方法》（GB/T 20277—2006）；

《网络脆弱性扫描产品测评方法》（GB/T 20280—2006）。

4．他类标准

（1）风险评估

《信息安全风险评估规范》（GB/T 20984—2007）。

（2）事件管理

《信息安全事件管理指南》（GB/Z 20985—2007）；

《信息安全事件分类分级指南》（GB/Z 20986—2007）；

《信息系统灾难恢复规范》（GB/T 20988—2007）。

2.2.2 相关标准与等级保护各工作环节的关系

相关标准与等级保护各工作环节的关系如图 2-2 所示。围绕信息安全等级保护安全建设整改工作，对有关标准进行说明。

1．基础标准

《计算机信息系统安全保护等级划分准则》是强制性国家标准，是等级保护的基础性标准，在此基础上制定出《信息系统通用安全技术要求》等技术类、《信息系统安全管理要求》、《信息系统安全工程管理要求》等管理类、《操作系统安全技术要求》等产品类标准，在相关标准的制定时起到了基础作用。

2．安全要求类标准

《基本要求》以及行业标准规范和细则构成了信息系统安全建设整改的安全需求。

（1）《信息系统安全等级保护基本要求》（以下简称《基本要求》）。该标准是在《计算机信息系统安全保护等级划分准则》、技术类标准和管理类标准基础上，总结几年的实践，结合当前信息技术发展的实际情况研究制定的，该标准提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施。

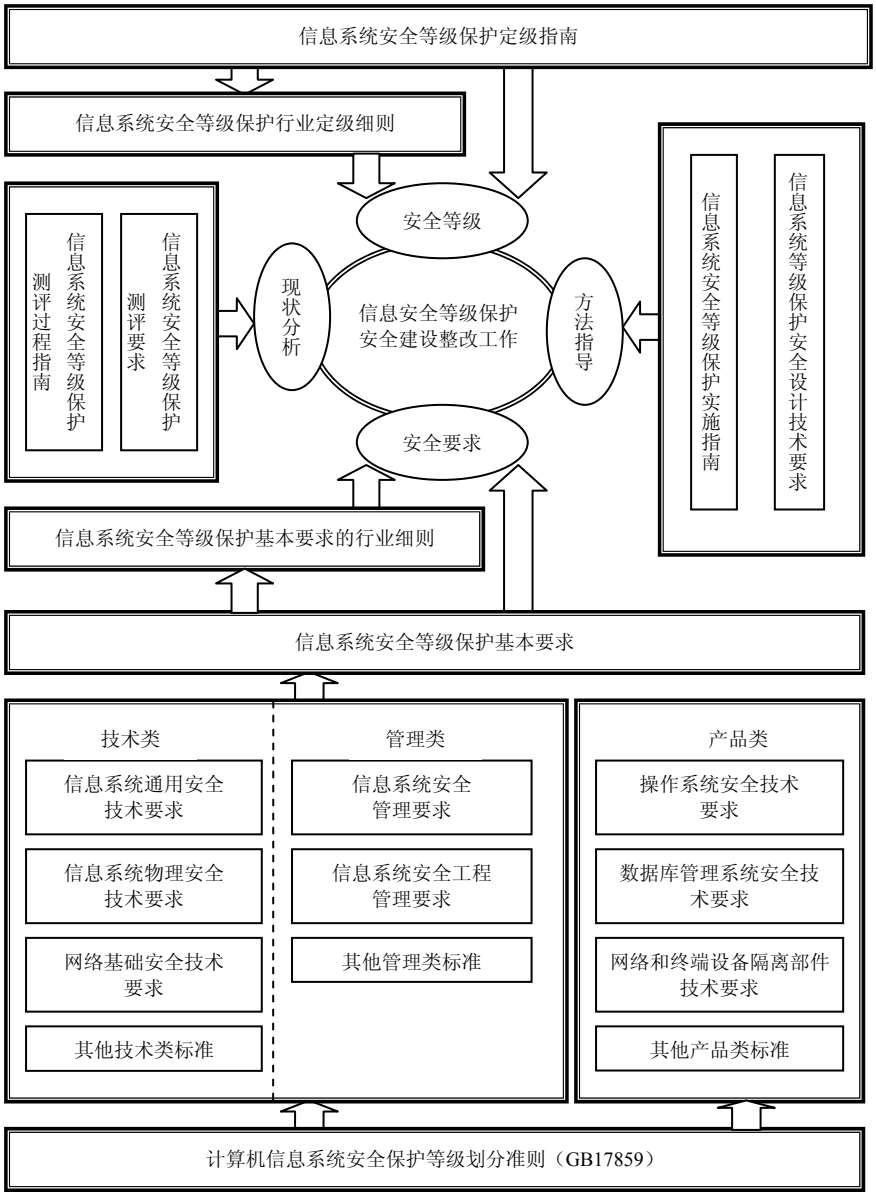

图 2-2　等级保护相关标准与等级保护各工作环节的关系

（2）信息系统安全等级保护基本要求的行业标准或细则。重点行业可以按照《基

本要求》等国家标准，结合行业特点，在公安部等有关部门指导下，确定《基本要求》的具体指标，在不低于《基本要求》的情况下，结合系统安全保护的特殊需求，制定行业标准规范或细则。

3．定级类标准

《信息系统安全等级保护定级指南》和信息系统安全等级保护行业定级细则为确定信息系统安全保护等级提供支持。

（1）《信息系统安全等级保护定级指南》（GB/T22240—2008）。该标准规定了定级的依据、对象、流程和方法以及等级变更等内容，用于指导开展信息系统定级工作。

（2）信息系统安全等级保护行业定级规范或细则。重点行业可以按照《信息系统安全等级保护定级指南》等国家标准，结合行业特点和信息系统的特殊性，在公安部等有关部门指导下，制定行业信息系统定级规范或细则。

4．方法指导类标准

《信息系统安全等级保护实施指南》和《信息系统等级保护安全设计技术要求》构成了指导信息系统安全建设整改的方法指导类标准。

（1）《信息系统安全等级保护实施指南》（信安字[2007]10 号）。该标准阐述了等级保护实施的基本原则、参与角色和信息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止等几个主要工作阶段中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

（2）《信息系统等级保护安全设计技术要求》（GB/T24856—2009）。该标准提出了信息系统等级保护安全设计的技术要求，包括第一级至第五级信息系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求，以及定级系统互联的设计技术要求，明确了体现定级系统安全保护能力的整体控制机制。该标准用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构等开展信息系统等级保护安全技术设计。

5．现状分析类标准

《信息系统安全等级保护测评要求》和《信息系统安全等级保护测评过程指南》构成了指导开展等级测评的标准规范。

（1）《信息系统安全等级保护测评要求》。该标准阐述了等级测评的原则、测评内容、测评强度、单元测评要求、整体测评要求、等级测评结论的产生方法等内容，用于规范和指导测评人员如何开展等级测评工作。

（2）《信息系统安全等级保护测评过程指南》。该标准阐述了信息系统等级测评的测评过程，明确了等级测评的工作任务、分析方法以及工作结果等，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动，用于规范测评机构的等级测评过程。

2.2.3 在应用有关标准中需要注意的几个问题

（1）《基本要求》是信息系统安全建设整改的基本目标，《信息系统等级保护安全设计技术要求》是实现该目标的方法和途径之一。《基本要求》中不包含安全设计和工程实施等内容，因此，在系统安全建设整改中，可以参照《信息系统安全等级保护实施指南》、《信息系统等级保护安全设计技术要求》和《信息系统安全工程管理要求》进行。

（2）由于信息系统定级时是根据业务信息安全等级和系统服务安全等级确定的系统安全等级，因此，在进行信息系统安全建设整改时，应根据业务信息安全等级和系统服务安全等级确定《基本要求》中相应的安全保护要求。各单位、各部门在进行信息系统安全建设整改方案设计时，要按照整体安全的原则，综合考虑安全保护措施，建立系统综合防护体系，提高系统的整体保护能力。

（3）《信息系统等级保护安全设计技术要求》依据《计算机信息系统安全保护等级划分准则》，从“计算环境安全、区域边界安全、通信网络安全和安全管理中心”

（一个中心三维防护）四个方面给出了五个级别信息系统安全保护设计的技术要求，用于指导信息系统等级保护安全技术设计。本标准不包括信息系统物理安全、安全管理、安全运维等方面的安全要求，所以应与《基本要求》等标准配合使用。

2.2.4 信息安全等级保护主要标准简要说明

现将信息安全等级保护标准体系中比较重要的《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护定级指南》、《信息系统安全管理要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》、《信息系统安全工程管理要求》、《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等十个标准作一简要说明。

1.《计算机信息系统安全保护等级划分准则》（GB17859—1999）

（1）主要用途

本标准对计算机信息系统的安全保护能力划分了五个等级，并明确了各个保护级别的技术保护措施要求。本标准是国家强制性技术规范，其主要用途包括：一是用于规范和指导计算机信息系统安全保护有关标准的制定；二是为安全产品的研究开发提供技术支持；三是为计算机信息系统安全法规的制定和执法部门的监督检查提供依据。

（2）主要内容

本标准界定了计算机信息系统的基本概念：计算机信息系统是由计算机及其相关和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

信息系统安全保护能力五级划分。信息系统按照安全保护能力划分为五个等级：第一级用户自主保护级，第二级系统审计保护级，第三级安全标记保护级，第四级

结构化保护级，第五级访问验证保护级。

从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面，采取逐级增强的方式提出了计算机信息系统的安全保护技术要求。

（3）使用说明

本标准是等级保护的基础性标准，其提出的某些安全保护技术要求受限于当前技术水平尚难以实现，但其构造的安全保护体系应随着科学技术的发展逐步落实。

2.《信息系统安全等级保护基本要求》（GB/T22239—2008）

（1）主要用途

根据《信息安全等级保护管理办法》的规定，信息系统按照重要性和被破坏后对国家安全、社会秩序、公共利益的危害性分为五个安全保护等级。不同安全保护等级的信息系统有着不同的安全需求，为此，针对不同等级的信息系统提出了相应的基本安全保护要求，各个级别信息系统的安全保护要求构成了《信息系统安全等级保护基本要求》（以下简称《基本要求》）。《基本要求》以《计算机信息系统安全保护等级划分准则》（GB17859—1999）为基础研究制定，提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施，为信息系统建设单位和运营使用单位在系统安全建设中提供参照。

（2）主要内容

《基本要求》）技术部分吸收和借鉴了 GB17859—1999 及相关标准，采纳其中的身份鉴别、数据完整性、自主访问控制、强制访问控制、审计、客体重用（改为剩余信息保护）标记、可信路径等 8 个安全机制，并将这些机制根据各级的安全目标，扩展到网络层、主机系统层、应用层和数据层，《基本要求》管理部分充分借鉴了 ISO/IEC 17799:2005 等国际上流行的信息安全管理方面的标准。

- 总体框架

《基本要求》分为基本技术要求和基本管理要求两大类，其中技术要求又分为物理安全、网络安全、主机安全、应用安全、数据安全及其备份恢复五个方面，管理要求又分为安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运行维护管理五个方面。

技术要求主要包括身份鉴别、自主访问控制、强制访问控制、安全审计、完整性和保密性保护、边界防护、恶意代码防范、密码技术应用等，以及物理环境和设施安全保护要求。

管理要求主要包括确定安全策略，落实信息安全责任制，建立安全组织机构，加强人员管理、系统建设和运行维护的安全管理。提出了机房安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、安全监测、备份与恢复管理、应急处置管理、密码管理、安全审计管理等基本安全管理制度要求，提出了建立岗位和人员管理制度、安全教育培训制度、安全建设整改的监理制度、自行检查制度等要求。

- 保护要求的分级方法

由于信息系统分为五个安全保护等级，其安全保护能力逐级增高，相应的安全保护要求和措施逐级增强，体现在两个方面：一是随着信息系统安全级别的提高，安全要求的项数增加；二是随着信息系统安全级别的提高，同一项安全要求的强度有所增加。例如，三级信息系统基本要求是在二级基本要求的基础上，在技术方面增加了网络恶意代码防范、剩余信息保护、抗抵赖等三项要求。同时，对身份鉴别、访问控制、安全审计、数据完整性及保密性方面的要求在强度上有所增加；在管理方面增加了监控管理和安全管理中心等两项要求，同时对安全管理制度评审、人员安全和系统建设过程管理提出了进一步要求。安全要求的项数和强度的不同，综合体现出不同等级信息系统安全要求的级差。

- 保护措施分类

技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中

部署软硬件并正确配置其安全功能来实现。根据保护侧重点的不同，技术类安全要求进一步细分为业务信息安全类要求（简记为 S）、服务保证类要求（简记为 A）和通用安全保护类要求（简记为 G）。信息安全类要求是指保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改；服务保证类要求是指保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用。管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面作出规定来实现。

（3）使用说明

- 《基本要求》对第一级信息系统的基本要求仅供用户参考，按照自主保护的原则采取必要的安全技术和管理措施。用户在进行信息系统安全建设整改时，可以在《基本要求》的基础上，根据行业和系统实际，提出特殊安全要求，开展安全建设整改。
- 《基本要求》给出了各级信息系统每一保护方面需要达到的要求，不是具体的安全建设整改方案或作业指导书，所以，实现基本要求的措施或方式并不局限于《基本要求》给出的内容，要结合系统自身的特点综合考虑采取的措施来达到基本要求提出的保护能力。
- 《基本要求》中不包含安全设计和工程实施等内容，因此，在系统安全建设整改中，可以参照《信息系统安全等级保护实施指南》、《信息系统等级保护安全设计技术要求》和《信息系统安全工程管理要求》进行。《基本要求》是信息系统安全建设整改的目标，《信息系统等级保护安全设计技术要求》是实现该目标的方法和途径之一。
- 《基本要求》综合了《信息系统物理安全技术要求》、《信息系统通用安全技术要求》和《信息系统安全管理要求》的有关内容，在进行系统安全建设整改方案设计时可进一步参考后三个标准。
- 由于系统定级时是根据业务信息安全等级和系统服务安全等级确定的系统安

全等级，因此，在进行系统安全建设时，应根据业务信息安全等级和系统服务安全等级确定《基本要求》中相应的安全保护要求，而通用安全保护要求要与系统等级对应。

- 信息系统运营使用单位在根据《基本要求》进行安全建设整改方案设计时，要按照整体安全的原则，综合考虑安全保护措施，建立并完善系统安全保障体系，提高系统的整体安全防护能力。

- 对于《基本要求》中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的，可以对基本安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

- 业务信息安全类（S 类）——关注的是保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改。如访问控制，该控制点主要关注的是防止未授权的访问系统，进而造成数据的修改或泄漏。至于对保证业务的正常连续运行并没有直接的影响。系统服务安全类（A 类）——关注的是保护系统连续正常的运行，避免因对系统的未授权修改、破坏而导致系统不可用。如资源控制，该控制点很好地体现了对业务正常运行的保护。通过对资源的使用限制、监视和预警等控制，保证了重要业务的正常运行。通用安全保护类（G 类）——既关注保护业务信息的安全性，同时也关注保护系统的连续可用性。大多数技术类安全要求都属于此类，保护的重点既是为了保证业务能够正常运行，同时数据要安全。如物理访问控制，该控制点主要是防止非授权人员物理访问系统主要工作环境，由于进入工作环境可能导致的后果既可能包括系统无法正常运行（如损坏某台重要服务器），也可能窃取某些重要数据。因此，它保护的重点二者兼而有之。

因此，在使用《基本要求》时，应该从信息系统的安全关注点出发，而信息系统的安全关注点可以从信息系统的定级结果中得到。有了定级结果，就可以选择和使用基本安全要求。举例来说，某信息系统定级结果为三级 S2A3G3 ，在选择和使用基本安全要求时应选择三级管理要求和 S2A3G3 的技术要求，可以分为以下过程：

一是选择《基本要求》中的第 7 章第三级基本要求，包括管理要求和技术要求；

二是根据定级结果 S2A3G3 进行调整。信息系统的业务信息安全保护等级为二级，系统服务安全保护等级为三级，因此，将第三级技术要求中的 S 类要求调整为第二级基本要求中的 S 类要求，第 1 一步中已选择的 A 类和 G 类基本要求保持不变；

三是根据行业要求或系统自身特点，分析需要增强的安全保护能力，需要增强业务信息安全保护能力的从三、四级的 S 类基本要求中选择，需要增强系统服务安全保护能力的从 4 级的 A 类基本要求中选择，整体需要增强的，则从四级 G 类基本要求中选择。在现有技术条件下，基本要求中的某些要求可能无法实现，如“对信息资源设置敏感标记”，信息系统运营、使用单位可以对基本要求进行调整，但是不能降低整体安全保护能力。

3.《信息系统安全等级保护实施指南》（信安字[2007]10 号）

（1）主要用途

《信息安全等级保护管理办法》（公通字[2007]43 号）第九条规定，信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。信息系统从规划设计到终止运行要经历几个阶段，《信息系统安全等级保护实施指南》（以下简称《实施指南》）用于指导信息系统运营使用单位，在信息系统从规划设计到终止运行的过程中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

（2）主要内容

- 总体框架

《实施指南》正文由 9 个章节构成：第 1～3 章定义了标准范围、规范性引用文件和术语定义。第 4 章介绍了等级保护实施的基本原则、参与角色和几个主要工作阶段。第 5～9 章对于信息系统定级、总体安全规划、安全设计与实施、安全运行与维护和信息系统终止五个工作阶段进行了详细描述和说明。本标准以信息系统安全等级保护建设为主要线索，定义信息系统等级保护实施的主要阶段和过程，包括信

息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止等五个阶段，对于每一个阶段，介绍了主要的工作过程和相关活动的目标、参与角色、输入条件、活动内容、输出结果等。

- 实施等级保护基本流程

对信息系统实施等级保护的基本流程如图 2-3 所示。

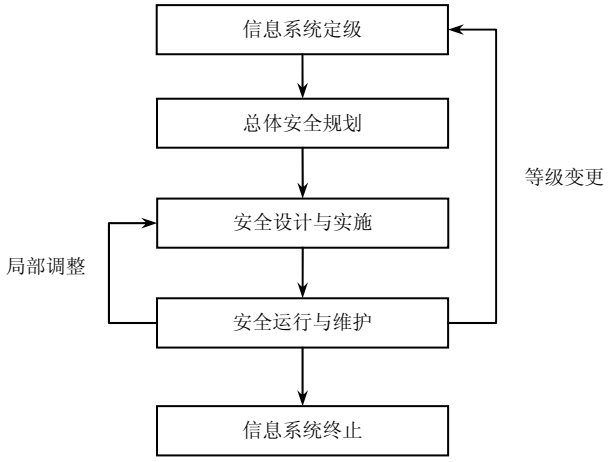

图 2-3　信息系统安全等级保护实施的基本流程

信息系统定级阶段内容。用于指导信息系统运营使用单位按照国家有关管理规范和《信息系统安全等级保护定级指南》，确定信息系统的安全保护等级。

总体安全规划阶段内容。用于指导信息系统运营使用单位根据信息系统定级情况，在分析信息系统安全需求的基础上，设计出科学、合理的信息系统总体安全方案，并确定安全建设项目规划，以指导后续的信息系统安全建设工程实施。

安全设计与实施阶段内容。用于指导信息系统运营使用单位按照信息系统安全总体方案的要求，结合信息系统安全建设项目计划，进行安全方案详细设计，实施安全建设工程，落实安全保护技术措施和安全管理措施。

安全运行与维护阶段内容。用于指导信息系统运营使用单位通过实施操作管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全评估和持续改进、等级测评以及监督检查等活动，进行系统运行的动态管理。

信息系统终止阶段内容。用于指导信息系统运营使用单位在信息系统被转移、终止或废弃时，正确处理系统内的重要信息，确保信息资产的安全。

另外，在安全运行与维护阶段，信息系统因需求变化等原因导致局部调整，而系统的安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全保护措施，确保满足等级保护的要求；当信息系统发生重大变更导致系统安全保护等级变化时，应从安全运行与维护阶段进入信息系统定级阶段，开始新一轮信息安全等级保护的实施过程。

（3）使用说明

本标准属于指南性标准，读者可通过该标准了解信息系统实施等级保护的过程、主要内容和脉络，不同角色在不同阶段的作用，不同活动的参与角色、活动内容等。

在实施等级保护的过程中除了参考本标准外，在不同阶段和环节中还需要参考和依据其他相关标准。例如在定级环节可参考《信息系统安全等级保护定级指南》。在系统建设环节可参考《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等。在等级测评环节可参照《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等。

4.《信息系统安全等级保护定级指南》（GB/T22240—2008）

（1）主要用途

《信息安全等级保护管理办法》（以下简称《管理办法》）对信息系统的安全保护等级给出了明确定义。信息系统定级是等级保护工作的首要环节，是开展信息系统安全建设整改、等级测评、监督检查等后续工作的重要基础。《信息系统安全等级保护定级指南》（以下简称《定级指南》）依据《管理办法》，从信息系统对国家安全、

经济建设、社会生活的重要作用，信息系统承载业务的重要性以及业务对信息系统的依赖程度等方面，提出确定信息系统安全保护等级的方法。

（2）主要内容

《定级指南》包括了定级原理、定级方法以及等级变更等内容。

- 定级原理

给出了信息系统五个安全保护等级的具体定义，将信息系统受到破坏时所侵害的客体和对客体造成侵害的程度等两方面因素作为信息系统的定级要素，并给出了定级要素与信息系统安全保护等级的对应关系。

- 定级方法

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级可以分别确定业务信息安全保护等级和系统服务安全保护等级，并取二者中的较高者为信息系统的安全保护等级。具体定级方法如图 2-4 所示。

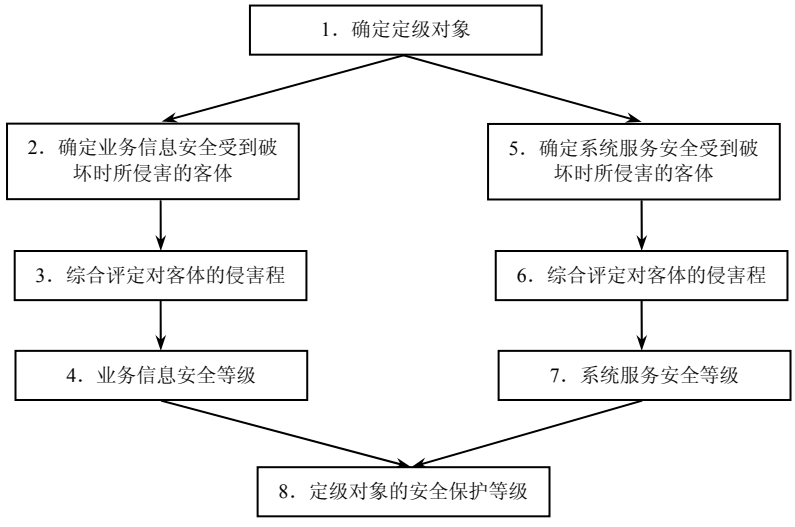

图 2-4　信息系统定级方法

- 等级变更

信息系统的安全保护等级会随着信息系统所处理信息或业务状态的变化而变化，当信息系统发生变化时应重新定级并备案。

（3）使用说明

应根据《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）要求，参照《定级指南》开展定级工作。

- 定级工作流程

可以参照以下步骤进行。

① 摸底调查，掌握信息系统底数。

② 确定定级对象。

③ 初步确定信息系统等级。

④ 专家评审。

⑤ 上级主管部门审批。

⑥ 到公安机关备案。

- 定级范围

新建信息系统和已经投入运行的信息系统（包括网络）都要定级。新建信息系统应在规划设计阶段定级，同步建设安全设施、落实安全保护措施。

- 等级确定

第一、二级信息系统为一般信息系统，第三、四、五级信息系统为重要信息系统。重要信息系统是国家和各部门保护的重点，国家在项目、经费、科研等方面将给予重点支持。信息系统的安全保护等级是信息系统的客观属性，在定级时，应站在维护国家信息安全的高度，综合考虑信息系统遭到破坏后对社会稳定的影响，确

定信息系统安全保护等级。具体可参考《信息安全等级保护工作简报》第 22 期。

- 定级工作指导

行业主管部门可以根据《定级指南》，结合行业特点和信息系统实际情况，出台定级指导意见，保证同行业信息系统在不同地区等级的一致性，指导本行业信息系统定级工作的开展。

5.《信息系统安全管理要求》（GB/T20269—2006）

（1）主要用途

《信息安全等级保护管理办法》明确规定，信息系统运营使用单位应当参照《信息系统安全管理要求》、《信息系统安全工程管理要求》、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。不同安全保护等级的信息系统有着不同的安全管理需求，为此，针对不同安全等级的信息系统提出了相应的安全管理要求。各个等级的安全管理要求构成了《信息系统安全管理要求》（以下简称《安全管理要求》）的基本内容。

《安全管理要求》为信息系统运营使用单位的信息系统安全管理策略制定、信息系统安全管理组织体系建设、信息系统安全管理制度体系建设、信息系统运维及规划建设管理、信息系统安全管理监督检查、信息系统安全管理体系建立和完善等提供指导和参考。在信息系统安全整改阶段进行信息系统等级保护安全管理方案设计的过程中，也可按照《安全管理要求》所规定的各个安全保护等级的安全管理要求，作为建立信息安全管理体系和制定相关信息安全管理制度、措施的基本依据。

（2）主要内容

- 总体框架

《安全管理要求》对当前信息系统安全普遍适用的安全管理进行了全面的描述，对信息和信息系统的安全保护提出了分等级安全管理的要求，阐述了安全管理要素及其强度，并将管理要求落实到信息安全等级保护所规定的五个等级上。《安全管理

要求》主要由 6 章和 2 个附录组成，其核心内容主要从以下八个方面描述：信息系统安全管理文档体系的建设要求；信息安全管理的组织保证，规定了信息安全管理的领导层、管理层以及执行机构的要求；信息系统安全管理中的风险管理要求；信息系统的环境和资源管理要求；信息系统的运行和维护管理要求；信息系统的业务连续性管理要求，提出备份与恢复、应急处理、安全事件处理的要求；信息系统的监督和检查管理要求；系统生存周期管理要求。

- 安全管理要求的分级描述方式

根据信息系统的五个安全保护等级的划分，随着信息系统安全保护能力逐级增高，相应的安全管理要求也逐级增强，体现在管理要素数量的增加和管理强度的增强两方面。例如，在描述信息系统安全管理要素“建立安全管理机构”时，在该安全管理要素的标题之下，首先简要说明本要素的作用，然后分列（a）配备安全管理人员、（b）建立安全职能部门、（c）成立安全领导小组、（d）主要负责人出任领导、（e）建立信息安全部门为小标题的五个不同强度的管理要求，而且在小标题之下还有更细化的描述。由（a）至（e）强度逐步提高，并明确规定不同安全等级应有选择地满足这些要求的一项。在具体描述时，有些管理要素的管理强度要求在前一强度基础之上继续完成的，会明确指出，如“在（a）的基础上，……”。

- 安全管理要素

《安全管理要求》以安全管理要素作为描述安全管理要求的基本组件。信息系统安全管理要素是指，为实现信息系统安全等级保护所规定的安全要求，从管理角度应采取的控制点，即实施的方法和措施。根据 GB 17859 对安全保护等级的划分，不同的安全保护等级会有不同的安全管理要求，具体体现在管理要素数量的增加和管理强度的增强两方面。这些安全管理要素构成信息系统安全管理的基本组件库，为提出分等级管理要求奠定了基础。安全管理要素的结构分为三个层次，为便于说明将第一层称为类，第二层称为族，第三层为具体的安全管理要素，共计 8 个类，30 个族，98 个要素，对于每个管理要素，根据特定情况分别列出不同的管理强度，最多分为五级，最少可不分级。

对信息系统安全管理要素分类划分为信息系统安全管理的日常措施、监督措施和保证措施等相互关联相互制约的三个方面。信息系统安全管理的日常措施包括环境和资源管理、运行和维护管理、业务连续性管理等 3 个类的安全管理要素；监督措施包括风险管理、监督和检查管理、生存周期管理等 3 个类的安全管理要素；保证措施包括策略和制度、机构和人员管理等 2 个类的安全管理要素。《安全管理要求》对于每个管理要素冠以不同编码和标题，以便在保护等级分解描述时引用方便；在安全管理要素不同强度的标题之后进行具体的描述。

- 安全管理分等级要求

《安全管理要求》表述了信息系统安全管理分等级要求，依据 GB 17859 划分的五个安全等级，分别对五个安全等级提出了信息系统安全管理要求。《安全管理要求》以信息系统安全管理的政策和制度、机构和人员管理、风险管理、环境和资源管理、操作和维护管理、应急和备份管理、业务连续性管理、监督和检查管理、生命周期管理等安全管理要素为基础，对每一个安全保护等级的信息系统的安全管理进行全面描述。还说明了信息系统安全管理要素及其强度与信息系统安全管理分等级要求的对应关系。

（3）使用说明

《安全管理要求》主要供下列三类人员使用。信息系统高层管理人员、信息系统使用管理人员和信息系统安全服务人员。

信息系统安全管理制度的制定。信息系统安全管理制度的制定要从实际出发，不要生搬硬套，而是遵循其思想和原则。

信息系统安全管理的评估和检查。《安全管理要求》可作为信息系统安全管理评估和检查的依据，具体评估和检查的实施方法，可进一步参考公共安全行业标准《信息安全技术 信息系统安全管理测评》（GA/T 713—2007）。

对于《安全管理要求》中提出的一些要求，从目前人员设置及组织机构的发展状况来看暂时还难以实现或者需要花费过高管理成本才能实现的安全管理要求，可

以采取一些其他的变通方法加以实现，但总的原则是保证不降低信息系统的整体安全保护能力。

6.《信息系统通用安全技术要求》（GB/T 20271—2006）

（1）主要用途

不同安全保护等级的信息系统具有相应的安全技术要求，各个等级的安全技术要求构成了《信息系统通用安全技术要求》的基本内容。本标准涉及组成各类信息系统的计算机系统、网络系统、应用软件系统及其所使用的信息技术产品和信息安全产品中所涉及的安全技术，其主要用途：一是为信息系统选择安全技术产品和设置安全设备的相应安全机制提供指导；二是为这些产品和设备的相关安全标准的制定提供参考。

（2）主要内容

- 总体框架

本标准以《计算机信息系统安全保护等级划分准则》（GB17859—1999）为基础研究制定，按安全技术要素，提出了与各个安全保护等级信息系统相对应的安全技术要素的安全性要求，并从安全功能和安全保证两个方面，对各安全技术要素应具有的安全性提出了要求。本标准由 6 章和 3 个附录组成。在第 1 章“范围”、第 2 章“规范性引用文件”以及第 3 章“术语、定义和缩略语”之后，第 4 章“安全功能技术要求”、第 5 章“安全保证技术要求”和第 6 章“信息系统安全技术分等级要求”，分别对相关内容进行描述，共涉及 40 个安全技术要素。其中安全功能技术要素 23 个，安全保证技术要素 17 个。

- 内容说明

安全功能技术要求。安全功能技术是指为使安全功能达到确定的安全目标应采取的技术措施。本标准第 4 章分别从物理安全、运行安全和数据安全等方面对所涉及的安全功能要素的安全技术要求进行了全面描述。

安全保证技术要求。安全保证技术是指为保证安全功能达到其安全性要求，从

设计、管理等方面所采取的技术措施。本标准第 5 章分别从安全子系统（SSOIS）自身安全保护、安全子系统设计和实现、安全子系统安全管理等方面对所涉及的安全保证要素的安全技术要求进行了全面描述。

安全技术分等级要求。按照五个安全保护等级的划分，在上述安全功能技术要求和安全保证技术要求的基础上，本标准第 6 章对第一级到第五级应达到的安全功能技术要求和安全保证技术要求分别进行了描述。为了便于读者了解较高一级与前一级的差别，对安全功能技术要求和安全保证技术要求安全要素的增加部分和安全性的增强部分用“宋体加粗”表示。

（3）使用说明

在开展信息系统等级保护安全建设整改工作中，应以《信息系统安全等级保护基本要求》为主，参照本标准落实安全管理制度和安全保护技术措施。

本标准按安全技术要素阐述了不同安全等级的安全技术要求，为信息系统在进行安全设计时选取相应安全等级的安全技术和安全产品提供参考，并不包含如何按照这些安全技术要求进行等级化信息系统安全设计、实现和工程实施等方面的内容，也不包括与信息系统安全运行管理相关的内容。

对于本标准中提出的暂时还难以实现或需要花费过高代价才能实现的安全技术要求，可以采取一些其他的变通方法加以实现，以达到信息系统所确定的安全保护要求，但总的原则是保证不降低信息系统的整体安全保护能力。

7.《信息系统等级保护安全设计技术要求》（GB/T24856—2009）

（1）主要用途

本标准依据《计算机信息系统安全保护等级划分准则》（GB17859—1999）规定的信息系统安全保护能力等级，以及配套系列标准的安全等级保护技术要求，给出了五个级别信息系统安全保护设计的技术要求，用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构等开展信息系统等级保护安全技术设计。

（2）主要内容

本标准提出了信息系统等级保护安全设计的技术要求，包括第一级至第五级信息系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求，以及定级系统互联的设计技术要求，明确了体现定级系统安全保护能力的整体控制机制。

- 总体框架

本标准第 4 章信息系统等级保护安全技术设计概述，以图示方式给出了信息系统等级保护安全技术设计框架。第 5 章到第 10 章分别对第一级至第五级系统安全保护环境设计和定级系统互联设计，从设计目标、设计策略和设计技术要求等方面进行了描述。附录 A 是对访问控制机制设计的描述，附录 B 是对第三级系统安全保护环境设计示例的描述。

- 定级系统安全保护环境设计主要内容

定级系统进行安全保护的环境由安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心构成。

安全计算环境。安全计算环境是对定级系统的信息进行存储、处理及实施安全策略的相关部件。安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。第三级安全计算环境从以下方面进行安全设计：用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、程序可信执行保护。

安全区域边界。安全区域边界是对定级系统的安全计算环境边界，以及在安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。第三级安全区域边界从以下方面进行安全设计：区域边界访问控制、区域边界包过滤、区域边界安全审计、区域

边界完整性保护。

安全通信网络。安全通信网络是对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。第三级安全通信网络从以下方面进行安全设计：通信网络安全审计、通信网络数据传输保密性保护、通信网络数据传输保密性保护、通信网络可信接入保护。

安全管理中心。安全管理中心是对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。第三级（含）以上的定级系统安全保护环境需要设置安全管理中心，分别称为第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。第二级信息系统可以选择配置第二级安全管理中心。安全管理中心设计主要从系统管理、安全管理和审计管理三方面考虑。

跨定级系统安全管理中心。跨定级系统安全管理中心是对相同或不同等级的定级系统之间互联的安全策略及安全互联部件上的安全机制实施统一管理的平台。跨定级系统安全管理中心设计技术要求：应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的系统管理、安全管理和审计管理。

（3）使用说明

本标准突出从“计算环境安全、区域边界安全、通信网络安全和安全管理中心”四个方面对信息系统进行安全技术设计。在安全设计中应注意各安全技术和机制之间的相互关联，通过对安全技术、机制和产品的有机集成，使信息系统安全保护技术能力符合其安全等级的保护要求。

本标准不包括信息系统物理安全、安全管理、安全运维等方面的安全要求，所以，在进行信息系统安全建设整改方案设计时，应与《信息系统安全等级保护基本要求》等标准配合使用。

信息系统安全建设整改的管理和技术目标是落实《信息系统安全等级保护基本要求》，而利用本标准进行信息系统安全技术设计是实现目标的方法之一。

8.《信息系统安全工程管理要求》（GB/T20282—2006）

（1）主要用途

不同安全保护等级的信息系统有着不同的安全工程管理需求，安全工程由安全等级、保证与实施要求两个维度组成，不同等级要求的安全工程对应不同的保证与实施要求。为此，针对不同等级信息系统的具体要求构成了安全工程管理要求体系。保证要求、实施要求、安全工程管理分等级要求和安全工程流程与安全工程要求构成了《信息系统安全工程管理要求》（以下简称《工程管理要求》）。《工程管理要求》以《计算机信息系统安全保护等级划分准则》为基础研究制定，规定了信息系统安全工程管理的不同要求，为信息系统建设的需求方、实施方与第三方工程实施在系统安全建设中提供参照，各方可以此为依据建立安全工程管理体系。

（2）主要内容

- 总体框架

《工程管理要求》分为保证要求和实施要求两大类，其中保证要求是由资格保证要求和组织保证要求构成，实施要求是由工程实施要求和项目实施要求构成。

资格保证要求包括系统集成资质、人员资质、第三方服务资质、安全产品资质、工程监理资质、法律法规政策符合性要求；组织保证要求包括定义组织的系统工程过程、改进组织的系统工程过程、过量系列产品演化、管理系统工程支持环境、培训、与供应商协调。

工程实施要求包括管理安全控制、评估影响、评估安全风险、评估威胁、评估脆弱性、建立保证论据、协调安全、监视安全态势、提供安全输入、指定安全要求、验证和确认安全性；项目实施要求包括质量保证、管理配置、管理项目风险、监视技术活动、计划及时活动。

- 基本关系

安全工程由安全等级、保证与实施要求两个维度组成，不同等级要求的安全工程对应不同的保证与实施要求。资格保证要求表示信息安全工程中对应具备一定能力级别的实施方或与工程相关第三方资质的要求；组织保证要求表示信息安全工程过程要求中对需求方组织保证的要求；工程实施要求表示信息安全工程中对安全实施过程的要求；项目实施要求表示信息安全工程中对项目实施过程的要求。

- 保护要求的分级方法

由于信息系统分为五个安全保护等级，其安全保护能力逐级增高，相应的安全工程管理要求逐级增强，体现在随着信息系统安全级别的提高，同一项安全工程管理要求的强度有所增加。例如，三级信息系统安全工程管理要求是在二级安全工程管理要求的基础上，在资格保证、组织保证、工程实施和项目实施的要求强度上都有所增加。在资格保证方面增加了对安全工程监理管理制度的要求；在组织保证方面增加了收集过程资产、确保关键组件的可用性等的要求；在工程实施方面增加了评估安全风险和威胁的可能性等的要求；在项目实施方面增加了沟通配置状况和分析项目问题等的要求。安全工程管理要求的强度不同，综合体现出不同等级信息系统安全工程管理要求的级差。

- 安全工程流程与安全工程要求

信息系统安全工程的全部流程可被划分为五个阶段，即：起始、设计、建设、运行和维护、废弃。安全保护的各级安全工程要求体现在安全过程的部分或全部阶段中，在全部安全工程要求中，组织保证要求和项目实施要求贯穿于项目实施的各个阶段，而资格保证要求和工程实施要求则与具体的一个或多个项目实施阶段有较强的联系。

（3）使用说明

《工程管理要求》不适用于涉密信息系统安全工程建设，对第一级信息系统的安全工程管理要求仅供用户参考，按照自主保护的原则制定安全工程管理体系。

《工程管理要求》给出了各级信息系统建设时在安全工程管理每一方面需要达到的要求，不是具体的安全工程管理体系，所以，实现安全工程管理要求的管理体系并不局限于《工程管理要求》给出的内容，要结合系统建设的特点综合考虑安全管理体系来达到安全工程管理要求提出的保障能力，用户还可以参考《信息化工程监理规范第 6 部分：信息化工程安全监理规范》。

《工程管理要求》综合了《信息技术安全性评估准则》、《信息安全管理实用规则》、《系统安全工程能力成熟度模型》和《信息处理系统 开放系统互连 基本参考模型》的有关内容，在进行系统安全工程管理体系建设时可进一步参考这些标准。

信息系统运行使用单位在根据《工程管理要求》进行安全工程管理体系建设时，要按照整体安全的原则，综合考虑安全保护措施，建立并完善系统安全保障及管理体系，提高安全工程的整体管理能力。

对于《工程管理要求》中提出的安全工程管理要求无法实现或有更加有效的安全管理要求可以替代的，可以对安全工程管理要求进行调整，调整的原则是保证不降低整体安全管理能力。

9.《信息系统安全等级保护测评要求》（报批稿）

（1）主要用途

根据《信息安全等级保护管理办法》的规定，信息系统建设完成后，运营使用单位或者其主管部门应当选择符合规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。《信息系统安全等级保护测评要求》（以下简称《测评要求》）依据《信息系统安全等级保护基本要求》规定了对信息系统安全等级保护进行安全测试评估的内容和方法，用于规范和指导测评人员的等级测评活动。

（2）主要内容

- 总体框架

本标准第 4 章介绍了等级测评的原则、测评内容、测评强度、结果重用和使用方法。第 5～9 章分别规定了对五个等级信息系统进行等级测评的单元测评要求。第 10 章描述了整体测评的四个方面，即安全控制间安全测评、层面间安全测评、区域间安全测评和系统结构测评安全测评。第 11 章描述了等级测评结论的产生方法。

- 测评方法和测评强度

本标准中的测评方法主要包括访谈、检查和测试等三种方法。测评机构对不同等级的信息系统需要实施相应强度的测试评估。测评强度反映在三种测评方法的广度和深度上。

- 单元测评

单元测评是针对《基本要求》内容进行的逐项测评，包括物理安全、网络安全、主机系统安全、应用安全和数据安全及备份恢复等五个安全技术层面以及安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个安全管理方面的内容。单元测评从测评指标、测评实施和结果判定等三个方面进行描述。

- 整体测评

整体测评是在单元测评的基础上进行的进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

（3）使用说明

《测评要求》针对等级测评提出了单元测评要求和整体测评要求，但未涉及工作过程、任务以及工作产品等内容，相关内容请参考《信息系统安全等级保护测评过程指南》。

测评人员在确定测评内容时，应依据被测信息系统的安全保护等级选择《测评要求》中对应的单元测评内容，并在相关测评结果的基础上实施整体测评。

测评结论的产生不能仅依据单项测评结果，而是应该在整体测评基础上，结合

被测系统的实际情况，综合评判信息系统是否具备对应等级的安全保护能力。

10.《信息系统安全等级保护测评过程指南》（报批稿）

（1）主要用途

根据《信息安全等级保护管理办法》的规定，信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。为规范等级测评机构的测评活动，保证测评结论准确、公正，《信息系统安全等级保护测评过程指南》（以下简称《测评过程指南》）明确了信息系统等级测评的测评过程，阐述了等级测评的工作任务、分析方法以及工作结果等，为信息系统测评机构、运营使用单位及其主管部门在等级测评工作中提供指导。

（2）主要内容

- 总体框架

《测评过程指南》以测评机构对三级信息系统的首次等级测评活动过程为主要线索，定义信息系统等级测评的主要活动和任务，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动等四个活动。其中测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项任务；方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评实施手册开发及测评方案编制六项任务；现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项任务；分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项任务。对于每一个活动，介绍了工作流程、主要的工作任务、输出文档、双方的职责等。对于各工作任务，描述了任务内容和输入/输出产品等。

- 等级测评工作流程。

等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测

评活动、分析及报告编制活动。而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

测评准备活动。测评准备活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。其主要任务是掌握被测系统的详细情况，为实施测评做好文档及测试工具等方面的准备。测评准备活动的基本工作流程及任务主要包括等级测评项目启动、信息收集和分析、工具和表单准备。

方案编制活动。方案编制活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。其主要任务是开发与被测信息系统相适应的测评内容、测评实施手册等，形成测评方案。方案编制活动的基本工作流程及任务如图 2-5 所示。

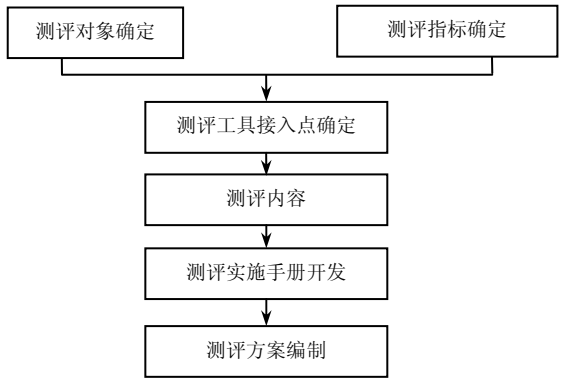

图 2-5　方案编制活动的基本工作流程及任务

现场测评活动。现场测评活动是开展等级测评工作的核心活动。其主要任务是按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评项目，包括单项测评和系统整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。现场测评活动的基本工作流程及任务主要包括现场测评准备、现场测评和结果记录、结果确认和资料归还。

分析与报告编制活动。分析与报告编制活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。其主要任务是根据现场测评结

果和《信息系统安全等级保护测评要求》（以下简称《测评要求》），通过单项测评结果判定和系统整体测评分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间的差距，综合评价被测信息系统保护状况，按照公安部制订的信息系统安全等级测评报告格式形成测评报告。分析与报告编制活动的基本工作流程及任务如图 2-6 所示。

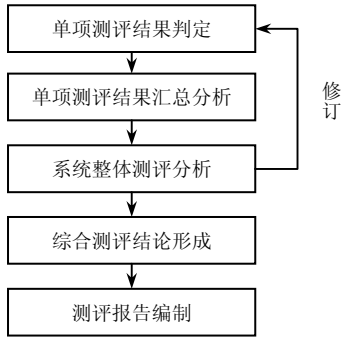

图 2-6　分析与报告编制活动的基本工作流程及任务

- 使用说明

《测评过程指南》给出了等级测评的基本工作过程、任务以及工作产品，不涉及等级测评中工作任务的具体执行方法和分析方法，所以用户需要参考和依据《测评要求》或其他相关标准自行开发测评方法和作业指导书。

《测评过程指南》针对已定级的信息系统给出等级测评工作过程，而且工作流程及任务是针对第三级信息系统的首次测评活动过程而言的，对于其他信息系统或再次实施等级测评的工作过程与该过程的差异及关系，应参考标准中的调整原则予以调整。

CHAPTER

3

第 3 章　信息系统定级与备案工作

本章主要介绍信息系统安全保护等级的确定，定级工作的流程和要求，备案工作的流程和要求等。

3.1　信息系统安全保护等级的划分与保护

3.1.1　信息系统定级工作原则

信息系统定级工作应按照“自主定级、专家评审、主管部门审批、公安机关审核”的原则进行。定级工作的主要内容包括：确定定级对象、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核，具体可按照《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字[2007]861 号）要求执行。各信息系统运营使用单位和主管部门是信息安全等级保护的责任主体，根据所属信息系统的重要程度和遭到破坏后的危害程度，确定信息系统的安全保护等级。同时，按照所定等级，依照相应等级的管理规范和技术标准，建设信息安全保护设施，建立安全制度，落实安全责任，对信息系统进行保护。

在等级保护工作中，信息系统运营使用单位和主管部门按照“谁主管谁负责，

谁运营谁负责”的原则开展工作，并接受信息安全监管部门对开展等级保护工作的监管。运营使用单位和主管部门是信息系统安全的第一责任人，对所属信息系统安全负有直接责任；公安、保密、密码部门对运营使用单位和主管部门开展等级保护工作进行监督、检查、指导，对重要信息系统安全负监管责任。由于重要信息系统的安全运行不仅影响本行业、本单位的生产和工作秩序，也会影响国家安全、社会稳定、公共利益，因此，国家必然要对重要信息系统的安全进行监管。

3.1.2 信息系统安全保护等级

信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。信息系统的安全保护等级分为五级，从第一级到第五级逐级增高。

3.1.3 信息系统安全保护等级的定级要素

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

1. 受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：一是公民、法人和其他组织的合法权益；二是社会秩序、公共利益；三是国家安全。

2. 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度有三种：一是造成一般损害；二是造成严重损害；三是造

成特别严重损害。

3.1.4 五级保护和监管

信息系统运营、使用单位依据国家信息安全等级保护政策和相关技术标准对信息系统进行保护，国家信息安全监管部门对其信息安全等级保护工作进行监督管理。定级要素与信息系统安全保护等级的关系如表 3-1 所示。

表 3-1 定级要素与安全保护等级的关系

等　级	对　象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

3.2 定级工作的主要步骤

信息系统定级是等级保护工作的首要环节和关键环节，是开展信息系统备案、建设整改、等级测评、监督检查等工作的重要基础。这里先明确一个概念，信息系统包括起支撑、传输作用的基础信息网络和各类应用系统。信息系统安全级别定级不准，系统备案、建设整改、等级测评等后续工作都会失去基础，信息系统安全就没有保证。定级工作可以按照下列步骤进行。

3.2.1 开展摸底调查

按照《定级工作通知》确定的定级范围，各单位、各部门可以组织开展对所属

信息系统进行摸底调查，摸清信息系统底数，掌握信息系统（包括信息网络）的业务类型、应用或服务范围、系统结构等基本情况，为下一步明确要求、落实责任奠定基础。

3.2.2 确定定级对象

在全国重要信息系统安全等级保护定级工作（以下简称“定级工作”）中，如何科学、合理地确定定级对象是最关键的问题。信息系统运营使用单位或主管部门按如下原则确定定级对象。

一是起支撑、传输作用的信息网络（包括专网、内网、外网、网管系统）要作为定级对象。但不是将整个网络作为一个定级对象，而是要从安全管理和安全责任的角度将基础信息网络划分成若干个最小安全域或最小单元去定级。

二是用于生产、调度、管理、作业、指挥、办公等目的的各类业务系统，要按照不同业务类别单独确定为定级对象，不以系统是否进行数据交换、是否独享设备为确定定级对象条件。不能将某一类信息系统作为一个定级对象去定级。

三是各单位网站要作为独立的定级对象。如果网站的后台数据库管理系统安全级别高，也要作为独立的定级对象。网站上运行的信息系统（例如对社会服务的报名考试系统）也要作为独立的定级对象。

四是确认负责定级的单位是否对所定级系统负有业务主管责任。也就是说，业务部门应主导对业务信息系统定级，运维部门（例如信息中心、托管方）可以协助定级并按照业务部门的要求开展后续安全保护工作。

五是具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件（如服务器、终端、网络设备等）作为定级对象。

例如，奥运网络主要包括，“奥组委办公外网”（承载自动化办公、场馆管理、

电子邮件、物流、员工之家等 16 项业务）、“奥组委内部办公局域网”（承载着财务管理、人事管理等 3 项业务）、“奥运票务网”（票务网站和票务管理系统）、“奥运官方网站”（门户网站和后台数据处理系统）、“奥运互联网接入”、“竞赛网”等六个奥运网络和信息系统。确定奥组委办公外网、奥组委内部办公局域网、票务网站、票务管理系统、奥运官方网站和竞赛网为定级对象。

3.2.3 初步确定信息系统等级

可以按照下列要求确定信息系统等级：

（1）定级责任主体。各信息系统运营使用单位和主管部门是信息系统定级的责任主体。

（2）定级要素。信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

信息系统的安全保护等级是信息系统本身的客观自然属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据，确定信息系统的安全保护等级。定级时应主要考虑信息系统破坏后对国家安全、社会稳定的影响，考虑境内外各种敌对势力、敌对分子针对重要信息系统入侵攻击破坏和窃取秘密等因素。既要防止个别单位片面追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。

（3）对各类系统定级的处理方法。一是单位自建的信息系统（与上级单位无关），单位自主定级。二是跨省或者全国统一联网运行的信息系统，可以由主管部门统一确定安全保护等级。其中：由各行业统一规划、统一建设、统一安全保护策略的全国联网系统，应由行业主管部门统一对下各级系统分别确定等级；由各行业统一规划、分级建设、全国联网的信息系统，应由部、省、地市分别确定系统等级，但各行业主管部门应对该类系统提出定级意见，避免出现同类系统下级定级比上级高的现象。对于该类系统的等级，下级确定后需报上级主管部门审批。

需特别注意的是：同类信息系统的安全保护等级不能随着部、省、市行政级别的降低而降低，例如地市级的重要行业的重要系统不能定为一、二级。

（4）新建系统的定级工作

对于新建系统，信息系统运营使用单位在规划设计时应确定信息系统安全保护等级，按照信息系统等级，同步规划、同步设计、同步实施安全保护技术措施和管理措施。有关信息系统安全保护等级确定的具体办法和要求见 3.3 节。

3.2.4 信息系统等级评审

信息系统运营使用单位或主管部门在初步确定信息系统安全保护等级后，为了保证定级合理、准确，可以聘请专家进行评审，并出具专家评审意见。

3.2.5 信息系统等级的审批

单位自建的信息系统（与上级单位无关），等级确定后，是否报上级主管部门审批，由各行业自行决定。信息系统运营使用单位参考专家定级评审意见，最终确定信息系统等级，形成《定级报告》。如果专家评审意见与运营使用单位意见不一致时，由运营使用单位自主决定系统等级，信息系统运营使用单位有上级主管部门的，应当经上级主管部门对安全保护等级进行审核批准。主管部门一般是指行业的上级主管部门或监管部门。如果是跨地域联网运营使用的信息系统，则必须由其上级主管部门审批，确保同类系统或分支系统在各地域分别定级的一致性。

3.2.6 公安机关审核

公安机关收到信息系统运营使用单位备案材料后，应对信息系统定级的准确性进行审核。公安机关的审核是定级工作的最后一道防线，应予以高度重视，严格把关。信息系统定级基本准确的，公安机关颁发由公安部统一监制的《信息系统安全

等级保护备案证明》（以下简称《备案证明》）。对于定级不准的，公安机关应向备案单位发整改通知，并建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。备案单位仍然坚持原定等级的，公安机关可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关同意后，同时通报备案单位上级主管部门。

3.3 如何确定信息系统安全保护等级

3.3.1 如何理解信息系统的五个安全保护等级

信息系统的安全保护等级是信息系统的客观属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据，确定信息系统的安全保护等级。既要防止个别单位片面追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。信息网络的安全等级可以参照在其上运行的信息系统的等级、网络的服务范围和自身的安全需求确定适当的保护等级，不以在其上运行的信息系统的最高等级或最低等级为标准，即不就高、不就低。

为了帮助信息系统运营使用单位准确确定信息系统安全保护等级，可以参考下列对五级的说明确定系统等级。

第一级信息系统：一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息系统。

第二级信息系统：一般适用于县级某些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。

第三级信息系统：一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨

省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这类系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省连接的网络系统等。

第四级信息系统：一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统。

第五级信息系统：一般适用于国家重要领域、重要部门中的极端重要系统。

3.3.2 定级的一般流程

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称为业务信息安全等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全等级。

确定信息系统安全保护等级的一般流程如下：确定作为定级对象的信息系统；确定业务信息安全受到破坏时所侵害的客体；根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度，根据业务信息的重要性和受到破坏后的危害性确定业务信息安全等级；确定系统服务安全受到破坏时所侵害的客体；根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度，根据系统服务的重要性和受到破坏后的危害性确定系统服务安全等级；由业务信息安全等级和系统服务安全等级的较高者确定定级对象的安全保护等级。上述步骤如图 3-1 所示。

1．确定受侵害的客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

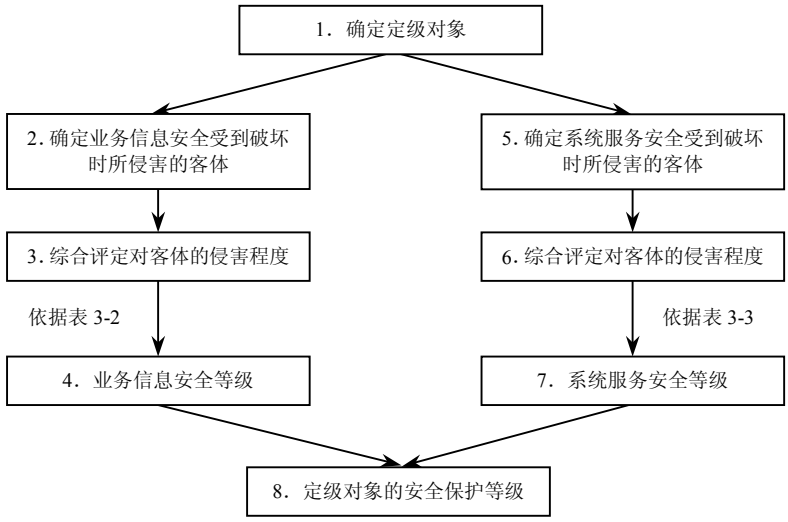

图 3-1　确定等级一般流程

侵害国家安全的事项包括以下方面：影响国家政权稳固和国防实力；影响国家统一、民族团结和社会安定；影响国家对外活动中的政治、经济利益；影响国家重要的安全保卫工作；影响国家经济竞争力和科技实力；其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：影响国家机关社会管理和公共服务的工作秩序；影响各种类型的经济活动秩序；影响各行业的科研、生产秩序；影响公众在法律约束和道德规范下的正常生活秩序等；其他影响社会秩序的事项。

影响公共利益的事项包括以下方面：影响社会成员使用公共设施；影响社会成员获取公开信息资源；影响社会成员接受公共服务等方面；其他影响公共利益的事项。

影响公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。

确定作为定级对象的信息系统受到破坏后所侵害的客体时，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

各行业可根据本行业业务特点，分析各类信息和各类信息系统与国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。

2．确定对客体的侵害程度

侵害的客观方面。在客观方面，对客体的侵害外在表现为对定级对象的破坏，其危害方式表现为对信息安全的破坏和对信息系统服务的破坏，其中信息安全是指确保信息系统内信息的保密性、完整性和可用性等，系统服务安全是指确保信息系统可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害方式。

信息安全和系统服务安全受到破坏后，可能产生以下危害后果：影响行使工作职能；导致业务能力下降；引起法律纠纷；导致财务损失；造成社会不良影响；对其他组织和个人造成损失；其他影响。

3．综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同，例如系统服务安全被破坏导致业务能力下降的程度可以从信息系统服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，应参照以下不同的判别基准：

如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；

如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的

总体利益作为判断侵害程度的基准。

不同危害后果的三种危害程度描述如下：

一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的资产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的资产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的资产损失，大范围的社会不良影响，对其他组织和个人造成非常严重的损害。

信息安全和系统服务安全被破坏后对客体的侵害程度，由对不同危害结果的危害程度进行综合评定得出。由于各行业信息系统所处理的信息种类和系统服务特点各不相同，信息安全和系统服务安全受到破坏后关注的危害结果、危害程度的计算方式均可能不同，各行业可根据本行业信息特点和系统服务特点，制定危害程度的综合评定方法，并给出侵害不同客体造成损害、严重损害、特别严重损害的具体定义。

4．确定信息系统安全保护等级

根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据如表 3-2 所示业务信息安全等级矩阵表，即可得到业务信息安全等级。

表 3-2　业务信息安全等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据如表 3-3 所示系统服务安全等级矩阵表，即可得到系统服务安全等级。

表 3-3　系统服务安全等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

作为定级对象的信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。定级对象等级确定后，可参照附录 C 中的《信息系统安全保护等级定级报告》模版起草定级报告。

例如，“奥组委办公内网”承载奥组委内部的人事、财务等业务，仅在奥组委少数部门内应用，不传输秘密信息和敏感信息。其受到破坏后，会影响内部办公，会对社会秩序、公共利益造成损害，定为二级；“奥组委办公外网”通过唯一出口与互联网相连，承载奥组委内部的电子邮件、物流、短信平台、场馆管理等业务，在奥组委总部范围应用，其受到破坏后，会对社会秩序、公共利益造成损害，定为二级。“票务网站”负责提供票务申请、信息填写等业务，采集购票者信息和订票信息，不与“票务管理系统”直接相连，其受到破坏后，会对社会秩序、公共利益造成损害，定为二级。“票务管理系统”存储处理通过各种方式申请、购买奥运票务的个人数据，是“票务网站”的核心，其受到破坏后，会对社会秩序、公共利益造成严重损害，定为三级。“奥运官方网站”承担在互联网上对外宣传、报道奥运重大事项，是北京奥运通过互联网对外宣传的门户，其服务保障性要求很高，受到破坏后，会对社会秩序、公共利益造成严重损害，定为三级。“竞赛网”承担赛事安排、计时、成绩统计等重大事项，其数据安全和服务保障性要求很高，受到破坏后，会对社会秩序、公共利益造成严重损害，定为三级。

3.4 信息系统备案工作的内容和要求

3.4.1 信息系统备案与受理

信息安全等级保护备案工作包括信息系统备案、受理、审核和备案信息管理等工作。信息系统运营使用单位和受理备案的公安机关应按照《信息安全等级保护备案实施细则》（公信安[2007]1360 号）的要求办理信息系统备案工作。

1．备案

第二级以上信息系统，在安全保护等级确定后 30 日内，由其运营、使用单位或者其主管部门（以下简称“备案单位”）到所在地设区的市级以上公安机关办理备案手续。办理备案手续时，应当首先到公安机关指定的网址下载并填写备案表，准备好备案文件，然后到指定的地点备案。

备案时应当提交《信息系统安全等级保护备案表》（以下简称《备案表》，参见附录 C）（一式两份）及其电子文档。第二级以上信息系统备案时需提交《备案表》中的表一、二、三；第三级以上信息系统还应当在系统整改、测评完成后 30 日内提交《备案表》表四及其有关材料。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续；其他信息系统向北京市公安局备案。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。各部委统一定级信息系统在各地的分支系统（包括终端连接、安装上级系统运行的没有数据库的分系统），即使是上级主管部门定级的，也要到当地公安网监备案。

2．受理备案

地市级以上公安机关公共信息网络安全监察部门受理本辖区内备案单位的备

案。隶属于省级的备案单位，其跨地（市）联网运行的信息系统，由省级公安机关公共信息网络安全监察部门受理备案。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由公安部公共信息网络安全监察局受理备案，其他信息系统由北京市公安局公共信息网络安全监察部门受理备案。

隶属于中央的非在京单位的信息系统，由当地省级公安机关公共信息网络安全监察部门（或其指定的地市级公安机关公共信息网络安全监察部门）受理备案。

跨省或者全国统一联网运行并由主管部门统一定级的信息系统在各地运行、应用的分支系统（包括由上级主管部门定级，在当地有应用的信息系统），由所在地地市级以上公安机关公共信息网络安全监察部门受理备案。

3．备案信息管理

公安部组织开发了重要信息系统安全监察管理系统，配发给各地，搭建一个部、省、市三级公安机关等级保护综合管理平台。该系统部、省两级公安机关部署，部、省、市三级公安机关应用，为全国信息系统定级、备案和监督检查工作提供支持，为重要信息系统安全监察业务服务。各地公安机关要按照《关于部署开展等级保护安全监察管理系统建设的通知》要求，组织本地开展系统建设，及时将定级备案和相关数据录入系统，利用该系统开展等级保护工作。

3.4.2 公安机关受理备案要求

（1）受理备案的公安机关公共信息网络安全监察部门应该设立专门的备案窗口，配备必要的设备和警力，专门负责受理备案工作，受理备案地点、时间、联系人和联系方式等应向社会公布。

（2）接收备案材料后，公安机关应当对下列内容进行审核：备案材料填写是否完整，是否符合要求，其纸质材料和电子文档是否一致；信息系统所定安全保护等

级是否准确。

（3）公安机关收到备案单位提交的备案材料后，对属于本级公安机关受理范围且备案材料齐全的，应当向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案材料不齐全的，应当当场或者在五日内一次性告知其补正内容；对不属于本级公安机关受理范围的，应当书面告知备案单位到有管辖权的公安机关办理。

（4）经审核符合等级保护要求的，公安机关应当自收到备案材料之日起的十个工作日内，将加盖本级公安机关印章（或等级保护专用章）的《备案表》一份反馈备案单位，一份存档；对不符合等级保护要求的，公安机关公共信息网络安全监察部门应当在十个工作日内通知备案单位进行整改，并出具《信息系统安全等级保护备案审核结果通知》。

（5）《备案表》中表一、表二、表三内容经审核合格的，公安机关出具《信息系统安全等级保护备案证明》（以下简称《备案证明》）。《备案证明》由公安部统一监制。

（6）受理备案的公安机关公共信息网络安全监察部门应当建立管理制度，对备案材料按照等级进行严格管理，严格遵守保密制度，未经批准不得对外提供查询。

3.4.3 对定级不准以及不备案情况的处理

（1）公安机关对定级不准的备案单位，在通知整改的同时，应当建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。

（2）备案单位仍然坚持原定等级的，公安机关可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关同意后，同时通报备案单位上级主管部门。

（3）对拒不备案的，公安机关应当依据《中华人民共和国计算机信息系统安全保护条例》等其他有关法律、法规规定，责令限期整改。逾期仍不备案的，予以警告，并向其上级主管部门通报。向中央和国家机关通报的，应当报经公安部同意。

CHAPTER

4

第 4 章　信息安全等级保护安全建设整改工作

本章主要介绍信息安全等级保护安全建设整改工作的目标、内容、方法、流程、要求等，以指导各单位、各部门开展信息安全等级保护安全建设整改工作。

4.1　工作目标和工作内容

4.1.1　工作目标

1．三年时间完成

由于一些重要行业信息系统较多，受资金、人员等条件限制，考虑实际情况，全国已定级信息系统安全建设整改工作总体上用三年时间（2012 年底前）完成。各行业主管（监管）部门应按照时间要求，根据本行业信息系统数量和实际情况，合理部署总体工作进度。

2．三项重点工作

通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评等三项重点工作，落实等级保护制度的各项要求。

3．达到五方面目标

通过开展安全建设整改工作，达到以下五方面目标：一是信息系统安全管理水平明显提高，二是信息系统安全防范能力明显增强，三是信息系统安全隐患和安全事故明显减少，四是有效保障信息化健康发展，五是有效维护国家安全、社会秩序和公共利益。

4.1.2 工作范围和工作特点

1．工作范围

目前，少数单位和部门尚未开展信息系统定级备案工作，存在漏定级、漏备案和定级不准等情况，所以，各行业主管（监管）部门应在公安部指导下出台行业信息系统定级指导意见和要求，先解决信息系统定级备案工作中存在的突出问题，在此基础上开展安全建设整改工作。开展安全建设整改工作的信息系统范围如下：一是各单位、各部门要将已备案的第二级（含）以上信息系统纳入安全建设整改的范围。二是尚未开展定级备案的信息系统，要先定级备案，再开展安全建设整改。三是新建系统要同步开展安全建设工作。

2．工作特点

安全建设整改工作与各单位、各部门在信息系统建设中开展的安全建设工作有联系又有区别，其主要特点主要体现在以下四个方面：

（1）继承发展。安全建设整改工作是在各单位、各部门信息系统安全保护工作的基础上开展的，是对原有工作的继承和发展。

（2）引入标准。各单位、各部门按照国家最新出台的一系列有关标准规范，从管理和技术两方面开展安全建设整改工作，将技术措施和管理措施有机结合，着重建立信息系统综合防护体系，提高信息系统整体安全保护能力。

（3）外部监督。传统的信息系统安全保护工作大多是自主、自愿行为，而信息

安全等级保护安全建设整改工作是有政府职能部门监督的行为。全国公安机关对各单位、各部门等级保护工作的开展进行监督、检查。

（4）政策牵引。公安机关会同国家保密部门、密码工作部门和信息化部门出台了一系列政策文件和工作指南，为各单位、各部门开展等级保护工作提供了一定的保障机制。

3．工作目的

在已定级的信息系统中，大多数信息系统在建设之初并没有将等级保护要求作为安全需求加以考虑，因此所构建的信息系统安全保护体系或采取的安全保护措施是以满足本部门、本单位的安全需求为出发点的。随着等级保护工作的逐步展开，尤其是在信息系统确定了安全保护定级之后，重新审视现有信息系统的安全保护状况，由于建设年代不同、所在地域差异、设计人员和实施人员的水平差距等都会造成其信息系统的保护水平参差不齐。

通过开展安全建设整改工作，使信息系统可以按照等级保护相应等级的要求进行设计、规划和实施，将国家的政策标准要求、机构的使命性要求、系统可能面临的环境和影响以及机构自身的需求相结合作为信息系统的安全需求，使具有相同安全保护等级的信息系统能够达到相应等级的基本保护水平和保护能力。

4．工作要求

自 2009 年起，各单位、各部门要对定级备案、等级测评、安全建设整改和自查等工作开展情况进行年度总结（见《关于报送 2009 年信息安全等级保护工作总结的函》（公信安[2009]1609 号）），于每年年底前报同级公安机关网安部门，各省（自治区、直辖市）公安机关网安部门报公安部网络安全保卫局。信息系统备案单位每半年要填写《信息安全等级保护安全建设整改工作情况统计表》并报受理备案的公安机关。

4.1.3 工作内容

各单位、各部门在组织开展信息系统定级时，是按照有关标准要求，对每个业

务系统进行定级，但在开展信息系统安全建设整改时，可以采取“分区、分域”的方法，按照“整体保护”的原则进行整改方案设计，对信息系统进行加固改造，缺什么补什么。对于新建系统，在规划设计时应确定信息系统安全保护等级，按照信息系统等级，同步规划、同步设计、同步实施安全保护技术措施。

1．信息安全等级保护安全管理制度建设

（1）开展安全管理制度建设的依据

按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的安全管理制度。

（2）开展安全管理制度建设的内容

一是落实信息安全责任制。成立信息安全工作领导机构，明确信息安全工作的主管领导。成立专门的信息安全管理部门或落实信息安全责任部门，确定安全岗位，落实专职人员或兼职人员。明确落实领导机构、责任部门和有关人员的信息安全责任。

二是落实人员安全管理制度。制定人员录用、离岗、考核、教育培训等管理制度，落实管理的具体措施。对安全岗位人员要进行安全审查，定期进行培训、考核和安全保密教育，提高安全岗位人员的专业水平，逐步实现安全岗位人员持证上岗。

三是落实系统建设管理制度。建立信息系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理制度，明确工作内容、工作方法、工作流程和工作要求。

四是落实系统运维管理制度。建立机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置等管理制度，制定应急预案并定期开展演练，采取相应的管理技术措施和手段，确保系统运维管理制度的有效落实。

（3）开展安全管理制度建设的要求

在具体实施过程中，可逐项建立管理制度，也可以进行整合，形成完善的安全

管理体系。要根据具体情况，结合系统管理实际，不断健全完善管理制度。同时，将管理制度与管理技术措施有机结合，确保安全管理制度得到有效落实。

建立并落实监督检查机制。备案单位定期对各项制度的落实情况进行自查，行业主管部门组织开展督导检查，公安机关会同主管部门开展监督检查。

2．开展信息安全等级保护安全技术措施建设

（1）开展安全技术措施建设的依据

按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，建设信息系统安全保护技术措施。

（2）开展安全技术措施建设的内容

结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施。在信息系统安全技术建设整改中，可以采取“一个中心、三维防护”（即一个安全管理中心和计算环境安全、区域边界安全和通信网络安全）的防护策略，实现相应级别信息系统的安全保护技术要求，建立并完善信息系统综合防护体系，提高信息系统的安全防护能力和水平。

（3）开展安全技术措施建设的要求

备案单位要开展信息系统安全保护现状分析，确定信息系统安全技术建设整改需求，制定信息系统安全技术建设整改方案，组织实施信息系统安全建设整改工程，开展安全自查和等级测评，及时发现信息系统中存在的安全隐患和威胁，进一步开展安全建设整改工作。

4.1.4 信息系统安全保护能力的目标

对信息系统采取安全措施是为了使信息系统具备一定的安全保护能力，这种安

全保护能力主要表现为能够应对威胁的能力，称为对抗能力。但在某些情况下，信息系统无法阻挡威胁对自身的破坏时，如果信息系统具有很好的恢复能力，那么即使遭到破坏，也能在很短的时间内恢复系统原有的状态。能够在一定时间内恢复系统原有状态的能力构成了信息系统的另一种安全保护能力——恢复能力。对抗能力和恢复能力共同构成了信息系统的安全保护能力。

将“能力”分级，是基于系统的保护对象不同，其重要程度也不相同，重要程度决定了系统所具有的能力也就有所不同。一般来说，信息系统越重要，应具有的保护能力就越高。因为系统越重要，其所伴随的遭到破坏的可能性越大，遭到破坏后的后果越严重，因此需要提高相应的安全保护能力。

根据不同级别信息系统的重要程度，提出不同强度的对抗能力和恢复能力，将这些能力细化成安全目标，而基本要求就是为了满足这些安全目标而提出的安全保护要求。如图 4-1 所示给出了不同等级信息系统的安全保护能力、安全目标与安全要求之间的映射关系。

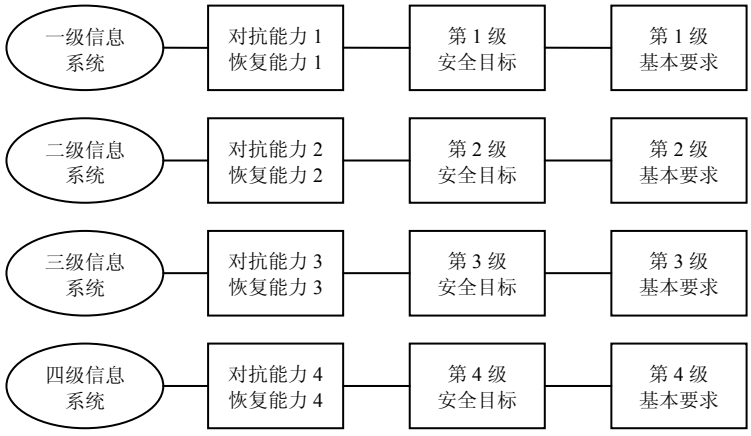

图 4-1　安全保护能力、安全目标与安全要求之间的映射关系

1．安全保护能力目标

各级信息系统应通过安全建设整改分别达到以下安全保护能力目标。

第一级信息系统：经过安全建设整改，信息系统具有抵御一般性攻击的能力，防范常见计算机病毒和恶意代码危害的能力；系统遭到损害后，具有恢复系统主要功能的能力。

第二级信息系统：经过安全建设整改，信息系统具有抵御小规模、较弱强度恶意攻击的能力，抵抗一般的自然灾害的能力，防范一般性计算机病毒和恶意代码危害的能力；具有检测常见的攻击行为，并对安全事件进行记录的能力；系统遭到损害后，具有恢复系统正常运行状态的能力。

第三级信息系统：经过安全建设整改，信息系统在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，抵抗较为严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能快速恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

第四级信息系统：经过安全建设整改，信息系统在统一的安全保护策略下具有抵御敌对势力有组织的大规模攻击的能力，抵抗严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行快速响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能立即恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

2．安全保护能力的实现

当信息系统包含的基本技术措施和基本管理措施，满足基本安全要求时，说明该信息系统具备了基本的安全保护能力，如图 4-2 所示。

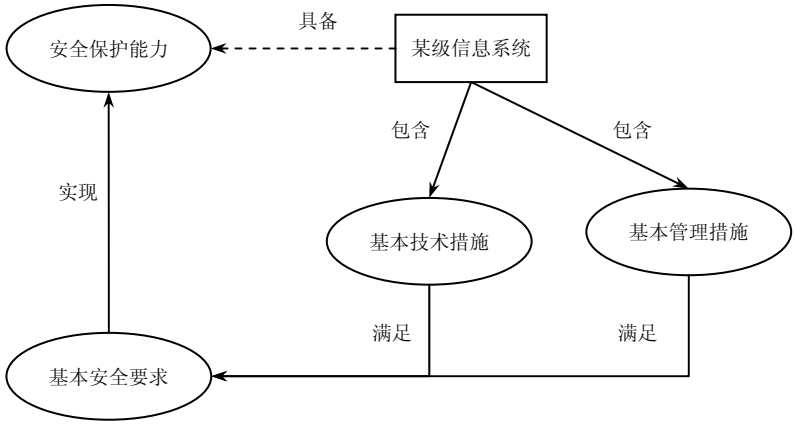

图 4-2　信息系统安全保护能力

4.1.5　基本要求的主要内容

信息系统运营使用单位在开展信息安全等级保护安全建设整改工作中，应按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系，提高信息系统整体安全保护能力。

1．基本要求主要内容

依据《信息系统安全等级保护基本要求》（以下简称《基本要求》），落实信息安全责任制，建立并落实各类安全管理制度，开展人员安全管理、系统建设管理和系统运维管理等工作，落实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，具体内容如图 4-3 所示。

需要说明的是：不同级别信息系统安全建设整改的具体内容应根据信息系统定级时的业务信息安全等级和系统服务安全等级，以及信息系统安全保护现状确定。信息系统安全建设整改工作具体实施可以根据实际情况，将安全管理和安全技术整改内容一并实施，或分步实施。

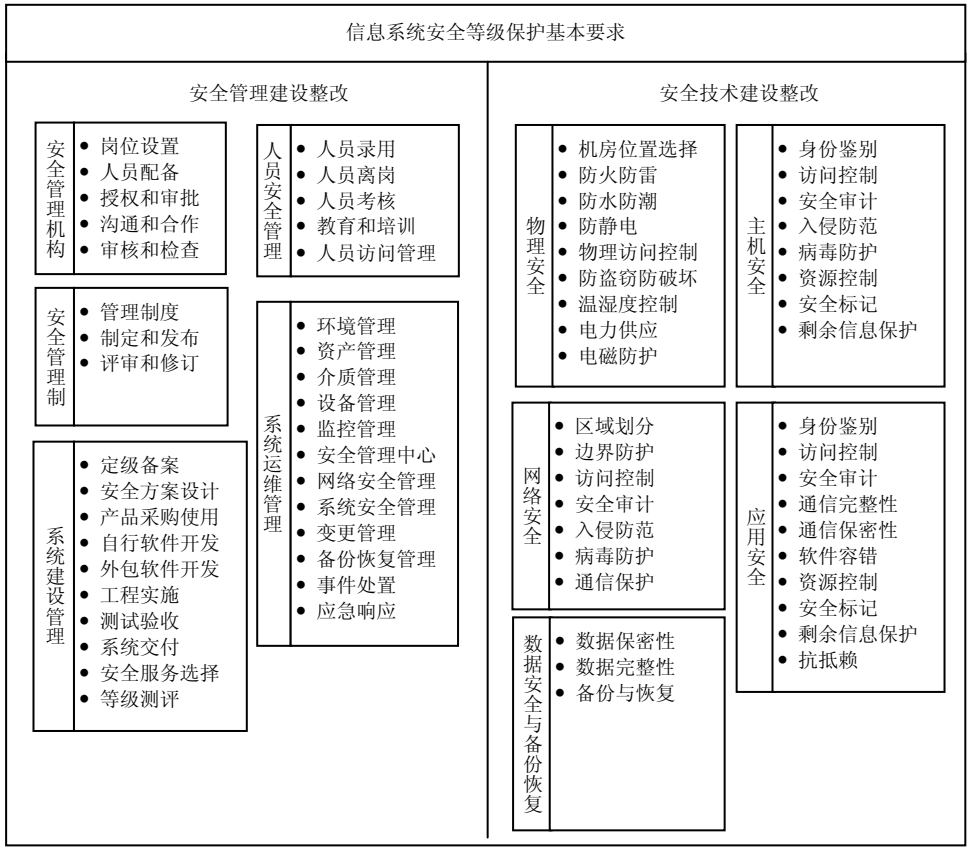

图 4-3　信息系统安全建设整改主要内容

2．各级信息系统安全保护技术措施要求

各级信息系统安全保护技术措施要求如表 4-1 所示。第二级到第四级信息系统安全保护技术措施要求都是在前一级要求的基础上，增加要求的项数或强度。

技术措施的特点：一级系统侧重于防护，二级系统侧重于防护和监测，三级系统侧重于策略、防护、监测和恢复，四级系统侧重于策略、防护、监测、响应和恢复。

表 4-1 各级信息系统安全保护技术措施要求

保护等级 / 技术措施	第一级	第二级	第三级	第四级
1. 身份鉴别和自主访问控制	要求身份鉴别，允许设置给其他用户共享资源，限制非授权访问	（同左）	（增加）采用两种以上身份识别技术要求	（同左）
2．强制访问控制			资源分类分级标记，按照访问控制策略控制用户访问的要求	（同左）
3．安全审计		对网络、主机、应用系统、用户行为进行审计记录	（增加）对审计的统计分析和报警；确保审计记录的可用，防止被非法访问和破坏。	（增加）违例行为终止要求
4. 完整性和保密性保护	数据和信息完整性要求	（增加）对信息加密、防泄露，可重用要求	（增加）对系统完整性要求，重要信息恢复要求	（同左）
5．边界防护		防止非授权外联要求	（增加）防止非授权接入、防止信息非授权交换	（同左）
6．资源控制		分配用户资源使用权限，保护主机和系统资源要求	（增加）对系统软硬件资源进行配置和检测，对违规使用行为进行报警要求	（增加）系统管理员配置和检测资源，安全管理员分配资源权限
7. 入侵防范和恶意代码防范	要求防范病毒等恶意代码	（增加）检测入侵攻击网络、系统行为要求	（增加）防范恶意代码入侵、植入、发作、传播要求，报警和清除要求	（增加）实时报警和清除措施
8．可信路径设置				要求建立安全通信路径
9．系统防渗透措施				要求重要应用程序隔离、数据结果可信验证，部件可信连接
10．安全管理平台设置			要求进行集中安全管理和控制	（同左）

续表

保护等级 / 技术措施	第一级	第二级	第三级	第四级
11．备份与恢复			要求系统资源本、异地备份，能够有效恢复	（同左）
12．密码技术应用			要求采用密码技术支持身份鉴别等其他安全功能	（同左）
13 环境和设施安全	要求基本的防水、火、雷、潮等，以及设备、设施、介质防盗防破坏	（增加）基本的电磁防护要求	（增加）出入口、内部环境电子设备监控，人员进出控制，增加环境安全防护强度，重要设备电子屏蔽	（同左）

3．各级信息系统安全保护管理措施要求

各级信息系统安全保护管理措施要求如表 4-2 所示。第二级到第四级信息系统安全保护管理措施要求都是在前一级要求的基础上，增加要求的项数或强度。

管理措施的特点：一级系统侧重于一般执行（部分活动建设制度），二级系统侧重于计划实施（主要过程建设制度），三级系统侧重于统一策略（管理制度体系化），四级系统侧重于持续改进（管理制度体系化/验证/改进）。

表 4-2　各级信息系统安全保护管理措施要求

保护等级 / 管理要求	第一级	第二级	第三级	第四级
1. 建立基本安全管理制度	要求建立网络安全、资产、设备、数据信息安全、用户管理、系统建设和运维等基本管理制度	（增加）制定信息安全工作策略、方案；备份与恢复，密码产品采购和使用管理制度；定期对制度进行评审和修订要求	（增加）制定信息安全规划，建立管理制度体系；增加机房、系统运维、风险管理、备份与恢复、密码管理制度要求	（增加）加强对有密级管理制度管理要求
2．落实安全责任制	要求设立安全管理岗位，落实责任，自行组织检查	（增加）设立安全主管；安全审计管理制度、岗位和人员管理制度	（增加）设立安全领导机构，建立安全职能部门，专职系统、网络、安全管理员和安全审计员	（增加）严格内部人员调离和保密义务，禁止外部人员访问关键区域要求

续表

保护等级 / 管理要求	第一级	第二级	第三级	第四级
3. 开展教育培训、考核	要求定期进行基本安全意识和责任教育培训	（增加）建立安全教育和培训制度，定期进行技能考核	（同左）	增加定期进行保密情况检查和考核要求
4. 建立等级测评、产品采购使用管理等制度		制定应急处置预案	（增加）等级测评和产品采购使用管理制度要求；系统建设整改制度化管理，事件报告和处置管理，定期开展应急处置演练要求	增加对重要设备进行专项测试要求；要求系统建设整改过程进行监理
5. 建设安全管理中心			要求制定规章制度和规程，设置安全管理员、安全审计员和系统管理员，分配相关权限，分别履行职责任务	（同左）

4.2 工作方法和工作流程

4.2.1 工作方法

（1）安全建设整改工作应以《基本要求》为基本目标，可以针对安全现状分析发现的问题进行加固改造，缺什么补什么；也可以进行总体安全建设整改设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，落实《基本要求》，最大程度发挥安全措施的保护能力。

（2）突出重点。建设过程中要突出重点，可以先对第三、四级信息系统开展安全建设整改，再对第二级系统开展整改；也可以对各等级系统同步规划实施，确保按期完成任务。

（3）试点示范。重点行业、部门可以根据需要和实际情况，选择有代表性的第二、三、四级信息系统先进行安全建设整改和等级测评工作试点、示范，在总结经

验的基础上全面推开。

（4）安全建设整改工作具体实施可以根据实际情况，将安全管理制度建设和安全技术措施建设内容一并实施，或分步实施。

（5）将安全建设整改工作与业务工作、信息化建设工作有机结合，利用信息安全等级保护综合工作平台，使等级保护工作日常化、常态化。

4.2.2 工作流程

安全建设整改工作可以分五步进行。

第一步：落实负责安全建设整改工作的责任部门，由责任部门牵头制定本单位和本行业信息系统安全建设整改工作规划，对安全建设整改工作进行总体部署。

第二步：开展信息系统安全保护现状分析，从管理和技术两个方面确定信息系统安全建设整改需求。可以依据《基本要求》等标准，采取对照检查、风险评估、等级测评等方法，分析判断目前所采取的安全保护措施与等级保护标准要求之间的差距，分析系统已发生的事件或事故，分析安全保护方面存在的问题，形成安全建设整改的需求并论证。

第三步：确定安全保护策略，制定信息系统安全建设整改方案。在安全需求分析的基础上，进行信息系统安全建设整改方案设计，包括总体设计和详细设计，制定工程预算和工程实施计划等，为后续安全建设整改工程实施提供依据。安全建设整改方案须经专家评审论证，第三级（含）以上信息系统安全建设整改方案应报公安机关备案，公安机关监督检查备案单位安全建设整改方案的实施。

第四步：按照信息系统安全建设整改方案，实施安全建设整改工程，建立并落实安全管理制度，落实安全责任制，建设安全设施，落实安全措施。在实施安全建设整改工程中，需要加强投资风险控制、实施流程管理、进度规划控制、工程质量控制和信息保密管理。

第五步：开展安全自查和等级测评，及时发现信息系统中存在的安全隐患和问

题，并通过风险分析，确定应解决的主要问题，进一步开展安全整改工作。

安全建设整改工作的具体步骤如图 4-3 所示。

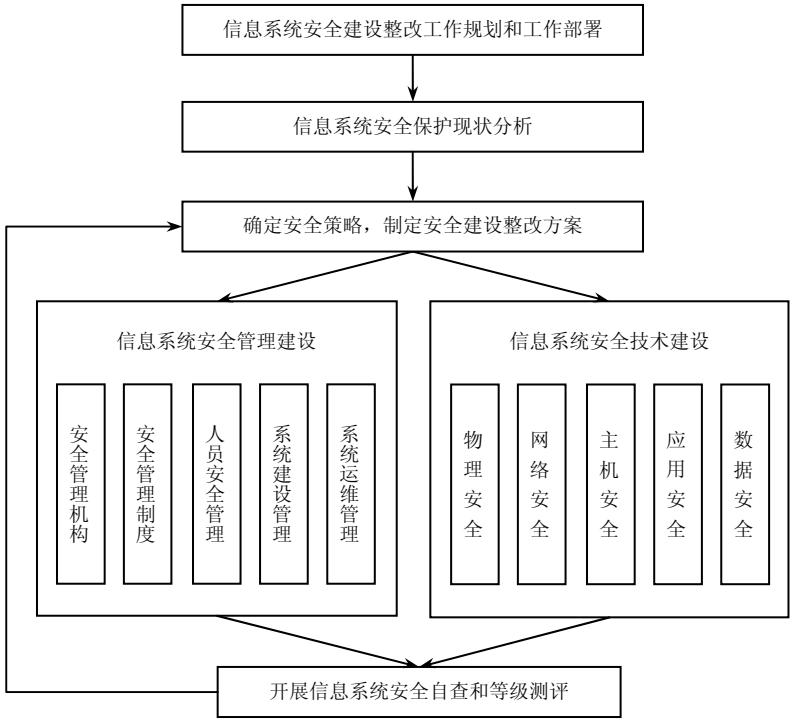

图 4-3　安全建设整改工作步骤

4.4　安全管理制度建设

按照国家有关规定，依据《基本要求》，参照《信息系统安全管理要求》等标准规范要求，开展信息系统等级保护安全管理制度建设工作。工作流程如图 4-4 所示。

4.4.1　落实信息安全责任制

明确领导机构和责任部门，设立或明确信息安全领导机构，明确主管领导，落

实责任部门。建立岗位和人员管理制度，根据职责分工，分别设置安全管理机构和岗位，明确每个岗位的职责与任务，落实安全管理责任制。建立安全教育和培训制度，对信息系统运维人员、管理人员、使用人员等定期进行培训和考核，提高相关人员的安全意识和操作水平。具体依据《基本要求》中的“安全管理机构”内容，同时可以参照《信息系统安全管理要求》等。

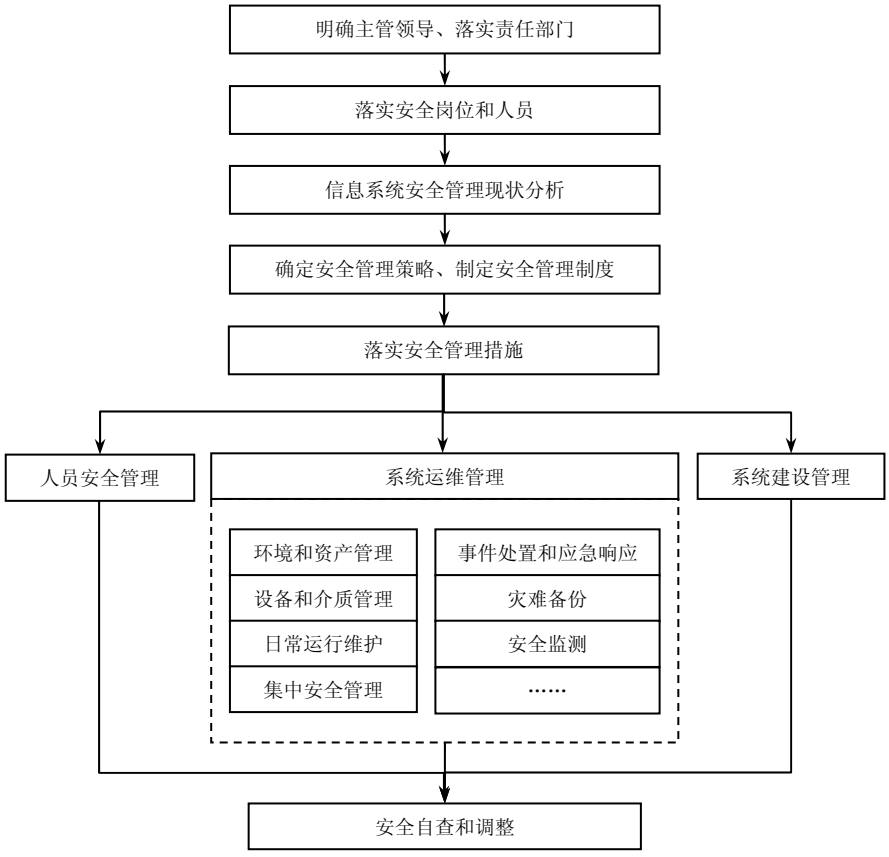

图 4-4　信息系统安全管理建设整改工作流程

落实安全责任制的具体措施还应参照执行相关管理规定，例如在党政机关信息系统应执行《关于加强党政机关计算机信息系统安全和保密管理的若干规定》，其中要求“各级应当明确一名主要领导负责计算机信息系统安全和保密工作，指定一个

工作机构具体负责计算机信息系统安全和保密综合管理。各部门内设机构应当指定一名信息安全保密员”。

4.4.2 信息系统安全管理现状分析

在开展信息系统安全管理建设整改之前，通过开展信息系统安全管理现状分析，查找信息系统安全管理建设整改需要解决的问题，明确信息系统安全管理建设整改的需求。

可以依据《基本要求》等标准，采取对照检查、风险评估、等级测评等方法，分析判断目前所采取的安全管理措施与等级保护标准要求之间的差距，分析系统已发生的事件或事故，分析安全管理方面存在的问题，形成安全管理建设整改的需求并论证。

对安全管理建设整改需求进行评审论证，该项工作可与安全技术建设整改需求论证工作一并进行。

4.4.3 制定安全管理策略和制度

根据安全管理需求，确定安全管理目标和安全策略，针对信息系统的各类管理活动，制定人员安全管理制度，明确人员录用、离岗、考核、教育培训等管理内容；制定系统建设管理制度，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理内容；制定系统运维管理制度，明确机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容；制定定期检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。规范安全管理人员或操作人员的操作规程等，形成安全管理体系（如图 4-5 所示）。具体依据《基本要求》中的“安全管理制度”内容，同时可以参照《信息系统安全管理要求》等标准。

安全管理体系规划的核心思想是调整原有管理模式和管理策略，既从全局高度

考虑为整个信息系统制定安全管理目标和统一的安全管理策略，又要从每个定级系统的实际等级、实际需求出发，选择和调整具体的安全管理措施，最后形成统一的系统整体安全管理体系。

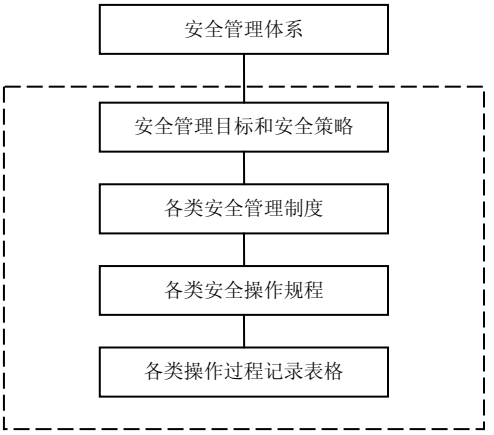

图 4-5　安全管理体系

4.4.4　落实安全管理措施

1．人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。规范人员录用、离岗、过程，关键岗位签署保密协议，对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对关键岗位的人员进行全面、严格的安全审查和技能考核。对外部人员允许访问的区域、系统、设备、信息等进行控制。具体依据《基本要求》中的“人员安全管理”内容，同时可以参照《信息系统安全管理要求》等。

2．系统运维管理

（1）环境和资产安全管理

明确环境（包括主机房、辅机房、办公环境等）安全管理的责任部门或责任

人，加强对人员出入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。对重要区域设置门禁控制手段，或使用视频监控等措施。明确资产（包括介质、设备、设施、数据和信息等）安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

（2）设备和介质安全管理

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面作出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

（3）日常运行维护

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理，制订相应的管理制度和操作规程并落实执行。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统安全管理要求》等。

（4）集中安全管理

第三级（含）以上信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息系统等级保护安全设计技术要求》和《信息系统安全管理要求》等。

（5）事件处置与应急响应

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等

级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。落实安全事件报告制度，第三级（含）以上信息系统发生较大、重大、特别重大安全事件时，运营使用单位应按照相应预案开展应急处置，并及时向受理备案的公安机关报告。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。具体依据《基本要求》中的“系统运维管理”内容，同时可以参照《信息安全事件分类分级指南》和《信息安全事件管理指南》等。

（6）灾难备份

要对第三级（含）以上信息系统采取灾难备份措施，防止重大事故、事件发生。识别需要定期备份的重要业务信息、系统数据及软件系统等，制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度。具体依据《基本要求》中的“系统运维管理”内容和《信息系统灾难恢复规范》。

（7）实时监测

开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为和业务应用等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，以便及时对安全事件进行响应与处置。具体依据《基本要求》中的“系统运维管理”。

（8）其他安全管理

对系统运行维护过程中的其他活动，如系统变更、密码使用等进行控制和管理。按国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

3．系统建设管理

系统建设管理的重点是与系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方、测评方、安全服务方等完成，运营使用单位人员的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、

方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等内容的管理责任部门、具体管理内容和控制方法，并按照管理制度落实各项管理措施。具体依据《基本要求》中的“系统建设管理”内容。

4.4.5 安全自查与调整

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。定期对信息系统安全状况进行自查，第三级信息系统每年自查一次，第四级信息系统每半年自查一次。经自查，信息系统安全状况未达到安全保护等级要求的，应当进一步开展整改。具体依据《基本要求》中的“安全管理机构”内容，同时可以参照《信息系统安全管理要求》等。信息系统安全管理建设整改工作完成后，安全管理方面的等级测评与安全技术方面的测评工作一并进行。

4.5 安全技术措施建设

按照国家有关规定，依据《基本要求》，参照《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，开展信息系统安全技术建设整改工作。工作流程如图 4-6 所示。

4.5.1 信息系统安全保护技术现状分析

了解掌握信息系统现状，分析信息系统的安全保护状况，明确信息系统安全技术建设整改需求，为安全建设整改技术方案设计提供依据。

1．信息系统现状分析

了解掌握信息系统的数量和等级、所处的网络区域以及信息系统所承载的业务应用情况，分析信息系统的边界、构成和相互关联情况，分析网络结构、内部区域、区域边界以及软、硬件资源等。具体可参照《信息系统安全等级保护实施指南》中

“信息系统分析”的内容。

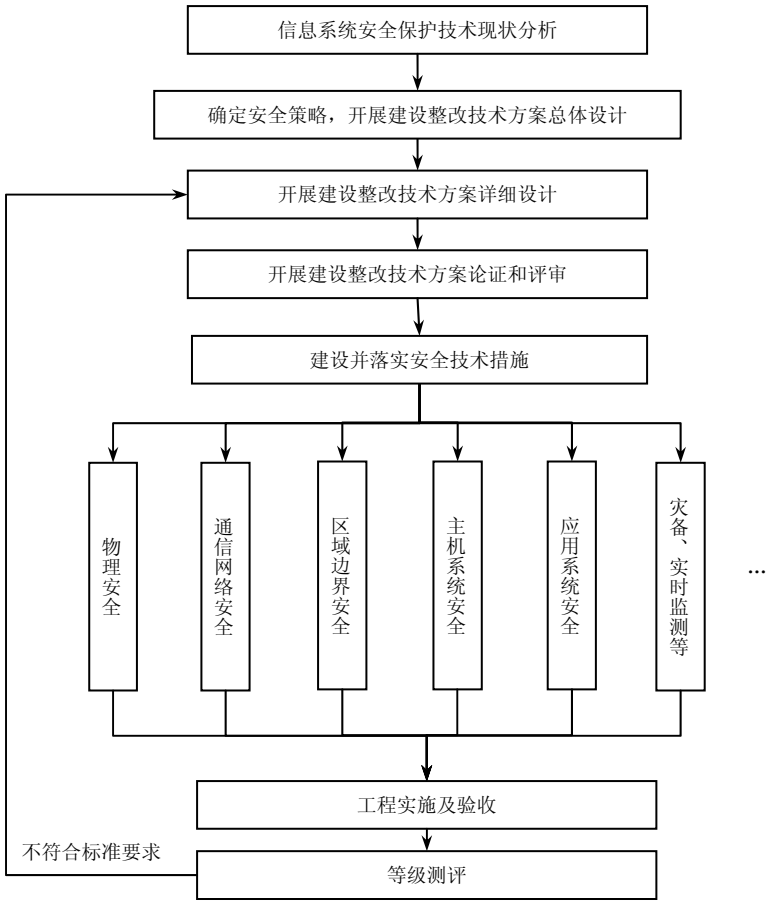

图 4-6　信息系统安全技术建设整改工作流程

2．信息系统安全保护技术现状分析

在开展信息系统安全技术建设整改之前，应通过开展信息系统安全保护技术现状分析，查找信息系统安全保护技术建设整改需要解决的问题，明确信息系统安全保护技术建设整改的需求。

可采取对照检查、风险评估、等级测评等方法，分析判断目前所采取的安全技

术措施与等级保护标准要求之间的差距，分析系统已发生的事件或事故，分析安全技术方面存在的问题，形成安全技术建设整改的基本安全需求。在满足信息系统安全等级保护基本要求的基础上，可以结合行业特点和信息系统安全保护的特殊要求，提出特殊安全需求。具体可参照《基本要求》、《信息系统安全等级保护测评要求》和《信息系统安全等级保护测评过程指南》等标准。

3．安全需求论证和确定

安全需求分析工作完成后，将信息系统的安全管理需求与安全技术需求综合形成安全需求报告。组织专家对安全需求进行评审论证。

4.5.2 信息系统安全技术建设整改方案设计

在安全需求分析的基础上，开展信息系统安全建设整改方案设计，包括总体设计和详细设计，制定工程预算和工程实施计划等，为后续安全建设整改工程实施提供依据。

1．确定安全技术策略，设计总体技术方案

（1）确定安全技术策略

安全技术策略是基于安全需求分析形成的纲领性的安全文件，包括安全工作的总体原则、安全策略等，用于指导信息系统安全技术体系和安全管理体系的构建。总体原则应该阐明安全工作的任务和总体目标，规定信息安全责任机构和职责，规定安全工作运行模式等。安全工作策略应说明安全组织机构设置策略、业务系统分级策略、数据信息分级策略、子系统互连策略、信息流控制策略等，用以指导系统安全技术体系结构设计。

（2）设计总体技术方案

在进行信息系统安全建设整改技术方案设计时，应以《基本要求》为基本目标，可以针对安全现状分析发现的问题进行加固改造，缺什么补什么；也可以进行总体的安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，

落实物理安全、网络安全、主机安全、应用安全和数据安全等方面的基本要求，最大程度发挥安全措施的保护能力。在进行安全技术设计时，可参考《信息系统等级保护安全设计技术要求》，从安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面落实安全保护技术要求。

2．安全技术方案详细设计

信息系统安全技术体系如图 4-7 所示。

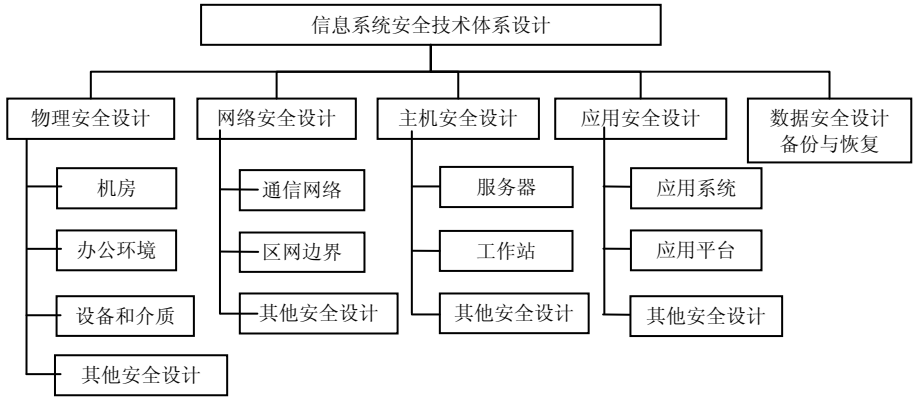

图 4-7　信息系统安全技术体系

（1）物理安全设计

从安全技术设施和安全技术措施两方面对信息系统所涉及的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括防震、防雷、防火、防水、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等方面。物理安全设计针对采用的安全技术设施或安全技术措施的物理部署、物理尺寸、功能指标、性能指标等内容提出具体设计参数。具体依据《基本要求》中的“物理安全”内容，同时可以参照《信息系统物理安全技术要求》等。

（2）通信网络安全设计

对信息系统所涉及的通信网络，包括骨干网络、城域网络和其他通信网络（租

用线路）等进行安全设计，设计内容包括通信过程数据完整性、数据保密性、保证通信可靠性的设备和线路冗余、通信网络的网络管理等方面。

通信网络安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置参数等提出具体设计细节。具体依据《基本要求》中“网络安全”内容，同时可以参照《网络基础安全技术要求》等。

（3）区域边界安全设计

对信息系统所涉及的区域网络边界进行安全设计，内容包括对区域网络的边界保护、区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码防范和网络设备自身保护等方面。

区域边界安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置策略和参数等提出具体设计细节。具体依据《基本要求》中的“网络安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《网络基础安全技术要求》等。

（4）主机系统安全设计

对信息系统涉及的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码防范、资源使用情况监控等。其中，安全配置细分为身份鉴别、访问控制、安全审计等方面的配置内容。具体依据《基本要求》中的“主机安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

（5）应用系统安全设计

对信息系统涉及的应用系统软件（含应用/中间件平台）进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错和资源控制等。应用系统安全设计需要关注应用系统的安全框架（含软件开发架构体系、访问控制模型、授权管理模型）、

安全机制选择与实现方式、编码安全规范与代码审核、产品部署形式以及安全参数/选项的配置。

在应用系统安全设计过程中，要确保应用系统安全是建立在操作系统、数据库管理系统安全基础之上的，其设计应同步考虑操作系统和数据库管理系统与之相关的内容。具体依据《基本要求》中的“应用安全”内容，同时可以参照《信息系统等级保护安全设计技术要求》、《信息系统通用安全技术要求》等。

（6）备份和恢复安全设计

针对信息系统的业务数据安全和系统服务连续性进行安全设计，设计内容包括数据备份系统、备用基础设施以及相关技术设施。针对业务数据安全的数据备份系统以考虑数据备份的范围、时间间隔、实现技术与介质以及数据备份线路的速率以及相关通信设备的规格和要求；针对信息系统服务连续性的安全设计可以考虑连续性保证方式（设备冗余、系统级冗余直至远程集群支持）与实现细节，包括相关的基础设施支持、冗余/集群机制的选择、硬件设备的功能/性能指标以及软硬件的部署形式与参数配置等。

备份和恢复的安全设计不是孤立的，是信息系统整体安全设计的有机部分，其安全措施的实现需要网络、主机和应用等多个层面安全机制的协同工作。备份和恢复安全设计要从业务影响分析入手，并同步考虑安全管理中与之对应的应急预案设计与演练、机构设置以及人力、物资资源管理等内容。具体依据《基本要求》中的“数据安全和备份恢复”内容，同时可以参照《信息系统灾难恢复规范》等。

3．建设经费预算和工程实施计划

（1）建设经费预算

根据信息系统的安全建设整改内容提出详细的经费预算，包括产品名称、型号、配置、数量、单价、总价和合计等，同时应包括集成费用、等级测评费用、服务费用和管理费用等。对于跨年度的安全建设整改或安全改建，提供分年度的经费预算。

（2）工程实施计划

根据信息系统的安全建设整改内容提出详细的工程实施计划，包括建设内容、工程组织、阶段划分、项目分解、时间计划和进度安排等。对于跨年度的安全建设整改或安全改建，要对安全建设整改方案明确的主要安全建设整改内容进行适当的项目分解，比如分解成机房安全改造项目、网络安全建设整改项目、系统平台和应用平台安全建设整改项目等，分别制定中期和短期的实施计划，短期内主要解决目前急迫和关键的问题。

4．方案论证和备案

将信息系统安全建设整改技术方案与安全管理体系规划共同形成安全建设整改方案。组织专家对安全建设整改方案进行评审论证，形成评审意见。第三级（含）以上信息系统安全建设整改方案应报公安机关备案，并组织实施安全建设整改工程。

4.5.3 安全建设整改工程实施和管理

1．工程实施和管理

安全建设整改工程实施的组织管理工作包括落实安全建设整改的责任部门和人员，保证建设资金足额到位，选择符合要求的安全建设整改服务商，采购符合要求的信息安全产品，管理和控制安全功能开发、集成过程的质量等方面。

按照《信息系统安全工程管理要求》中有关资格保障和组织保障等要求组织管理等级保护安全建设整改工程。实施流程管理、进度规划控制和工程质量控制可参照《信息系统安全工程管理要求》中第 8、第 9、第 10 章提出的工程实施、项目实施和安全工程流程控制要求，实现相应等级的工程目标和要求。

2．工程监理和验收

为保证建设工程的安全和质量，第二级（含）以上信息系统安全建设整改工程可以实施监理。监理内容包括对工程实施前期安全性、采购外包安全性、工程实施

过程安全性、系统环境安全性等方面的核查。

工程验收的内容包括全面检验工程项目所实现的安全功能、设备部署、安全配置等是否满足设计要求，工程施工质量是否达到预期指标，工程档案资料是否齐全等方面。在通过安全测评或测试的基础上，组织相应信息安全专家进行工程验收。具体参照《信息系统安全工程管理要求》。

3．安全等级测评

信息系统安全建设整改完成后要进行等级测评，在工程预算中应当包括等级测评费用。对第三级（含）以上信息系统每年要进行等级测评，并对测评费用做出预算。

在公安部备案的信息系统，备案单位应选择国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评；在省（区、市）、地市级公安机关备案的信息系统，备案单位应选择本省（区、市）信息安全等级保护工作协调小组办公室或国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评。

4.5.4 信息系统安全建设整改方案要素

以下整改方案的设计要素主要是针对单个信息系统的，也可参照针对整个单位或多个信息系统的整改方案进行设计。信息系统安全建设整改方案可以包含以下内容。

1．项目背景

简述信息系统概况，信息系统在等级保护工作方面的进展情况，例如定级备案情况和安全现状测评情况。

2．开展信息系统安全建设整改的法规、政策和技术依据

列举在建设整改工作中所依据的信息安全等级保护有关法规、政策、文件和信息安全等级保护技术标准。

3．信息系统安全建设整改安全需求分析

从技术和管理两方面描述信息系统建设情况、系统应用情况及安全建设情况。结合安全现状评估结果，分析信息系统现有保护状况与等级保护要求的差距，结合信息系统的自身安全需求形成安全建设整改安全需求。

4．信息系统安全等级保护建设整改技术方案设计

根据安全需求，确定整改技术方案的设计原则，建立总体技术框架结构，可以从物理环境、通信网络、计算环境、区域边界、安全管理中心等方面设计落实基本技术要求的物理、网络、系统、应用和数据的安全要求的技术路线。

5．信息系统安全等级保护建设整改管理体系设计

根据安全需求，确定整改管理体系的建设原则和指导思想，涉及安全管理策略和安全管理制度体系及其他具体管理措施。

6．信息系统安全产品选型及技术指标

依据整改技术设计，确定设备选型原则和部署策略，给出各类安全产品的选型指标和部署图，为设备采购提供依据。

7．安全整改后信息系统残余风险分析

安全整改可能不能解决所有不符合项目的问题，对于没有解决的问题，分析其可能的风险，提出风险规避措施。

8．信息系统安全等级保护整改项目实施计划

安全整改项目的实施需要制定相应的实施计划，落实项目管理部门和人员，对设备招标采购、工程实施协调、系统部署和测试验收、人员培训等活动进行规划安排。

9．信息系统安全等级保护项目预算

根据本单位信息化的中长期发展规划和近期的建设投资预算，将等级保护安全整改建设工作纳入整体规划，可以分期分批、有计划地实施建设整改，因此需要对建设项目进行费用预算，预算项目不仅包括安全设备投入，还应根据需要考虑集成费用、等级测评费用、服务费用和运行管理费用等。

4.6 信息安全产品的选择使用

4.6.1 选择获得销售许可证的信息安全产品

依据《中华人民共和国计算机信息系统安全保护条例》（国务院第 147 号令）、《计算机信息系统安全专用产品检测和销售许可证管理办法》（公安部第 32 号令）、《计算机病毒防治管理办法》（公安部第 51 号令）的有关规定，公安部网络安全保卫局依法对信息安全产品实行销售许可管理。进入我国市场销售的信息安全产品，首先需要经过公安部计算机信息系统安全产品质量监督检验中心和天津病毒产品检测中心的检测合格，并获得公安部颁发的销售许可证。各单位、各部门在安全建设整改工作中，应采购使用获得销售许可证的信息安全产品。

4.6.2 产品分等级检测和使用

2009 年公安部发布了《关于调整更新计算机信息系统安全专用产品检测执行标准规范的公告》（公信安[2009]1157 号），对信息安全产品依据分级的标准规范（29 类产品分级标准）开展分级检测工作。对于检测通过的产品，产品销售许可证书标注产品分级信息。各单位、各部门在进行安全建设整改时，应根据信息系统安全需求选择使用相应等级的产品。

4.6.3 第三级以上信息系统使用信息安全产品问题

《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）规定，“对信息系统中使用的信息安全产品实行按等级管理”。《管理办法》规定第三级以上信息系统应当选择使用我国自主研发的信息安全产品。信息安全产品是信息系统安全的重要基础，信息安全产品的使用和管理是国家信息安全等级保护制度的重要组成部分，尤其是进入到基础信息网络和重要信息系统中的信息安全产品将直接影响信息系统安全，甚至危及国家安全、社会稳定。因此，各单位、各部门应在满足使用要求的前提下，优先选择国产品。国家信息安全监管部门对进入第三级以上信息系统中使用的信息安全产品进行管理。

CHAPTER

5

第5章　信息安全等级保护等级测评工作

本章主要介绍等级测评工作的内容、方法、流程，以及等级测评机构的选择、等级测评报告编制等。

5.1　等级测评工作概述

5.1.1　等级测评的基本含义

信息系统安全等级保护测评工作（以下简称“等级测评”）是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对未涉及国家秘密的信息系统安全等级保护状况进行检测评估的活动。等级测评是标准符合性评判活动，即依据信息安全等级保护的国家标准或行业标准，按照特定方法对信息系统的安全保护能力进行科学公正的综合评判过程。

为加强对测评机构及测评人员管理，稳步推进等级测评机构建设，规范等级测评活动，提高测评机构、人员的技术能力和水平，公安部在总结等级保护测评体系建设试点工作的基础上，向各地公安机关下发了《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号），在全国组织开展信息

安全等级保护等级测评体系建设工作，以保障等级保护工作的顺利开展。根据通知精神，国家信息安全等级保护工作协调小组办公室负责受理隶属国家信息安全职能部门和重点行业主管部门申请单位提出的申请受理、审核推荐和监督检查等工作，各省级信息安全等级保护工作协调（领导）小组办公室（以下简称“省级等保办”）负责等级测评机构的申请受理、审核推荐和监督检查等工作。公安部信息安全等级保护评估中心（以下简称“评估中心”）负责测评机构的能力评估和培训工作。

5.1.2 等级测评的目的

根据《管理办法》的规定，信息系统按照《基本要求》等技术标准建设完成后，运营使用单位应当选择符合规定条件的测评机构，定期对信息系统安全等级状况开展等级测评。通过测评，一是可以掌握信息系统的安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；二是衡量信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。等级测评结果也是公安机关等安全监管部门进行监督、检查、指导的参照。

5.1.3 开展等级测评的时机

1. 安全建设整改前

在开展信息系统安全建设整改之前，信息系统运行使用单位可以通过等级测评（此时称为安全现状测评）分析判断目前信息系统所采取的安全措施与等级保护标准要求之间的差距，分析安全方面存在的问题，查找信息系统安全保护建设整改需要解决的问题，形成安全建设整改的安全需求。

2. 安全建设整改后

信息系统安全建设整改完成后，信息系统运行使用单位应通过等级测评对信息系统的等级保护措施落实情况与《基本要求》的要求之间的符合程度进行评判，形成信息系统安全等级测评报告。如果发现问题将继续整改。

3．定期开展等级测评

信息系统运行维护期间，应定期进行安全等级测评，及时发现和分析信息系统存在的安全问题。《管理办法》要求信息系统建设完成后，运营使用单位应当选择符合规定条件的测评机构，依据《测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级以上信息系统应当每年至少进行一次等级测评，对于重要部门的第二级信息系统，可以参照上述要求开展等级测评工作。

5.1.4 等级测评机构的业务范围

按照《信息安全等级保护测评工作管理规范》，测评机构有三类：由国家信息安全等级保护工作协调小组办公室推荐的信息安全职能部门测评机构、行业性测评机构，以及由省级等保办推荐的地方性测评机构。各类测评机构的业务范围划分和工作机制如下。

（1）信息安全职能部门测评机构可不受地域限制，在全国范围内开展测评业务，到地方开展测评时，应当事先告知属地省级等保办。

（2）行业测评机构原则上在本行业内开展测评，到地方开展测评时，应与属地省级等保办协调。行业性测评机构也可以承担其他行业信息系统的测评任务。

（3）地方性测评机构原则上在本地开展测评工作，也可以到异地开展测评，但事先须与当地等保办协调。地方性测评机构也可以承担中央、国家机关信息系统的测评任务。

（4）对测评工作中存在的其他特殊情况，应当在上述规定下，以受理备案的公安机关为主进行协调。

省级（含）以下备案单位可以在本省信息安全等级保护工作协调（领导）小组办公室发布的《信息安全等级保护测评机构推荐目录》中选择测评机构。省级以上各备案单位可以在国家信息安全等级保护工作协调小组办公室发布的《全国信息安

全等级保护测评机构推荐目录》中选择测评机构。没有测评机构的省（市）可以在《全国信息安全等级保护测评机构推荐目录》中选择测评机构。有关测评机构的申请、审核、推荐等工作详见 5.2 节。

5.1.5 等级测评依据的标准

测评机构应当依据《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等国家标准进行等级测评，按照公安部统一制订的《信息系统安全等级测评报告模版》（公信安[2009]1487 号）格式出具测评报告。按照行业标准规范开展安全建设整改的信息系统，可以国家标准为依据开展等级测评，也可以行业标准规范为依据开展等级测评。

《测评要求》与《基本要求》相适应，提出了测评指标、测评实施和结果判定三部分内容。测评指标直接指向《基本要求》相应等级的基本要求，在内容上，测评指标与相应的基本要求完全一致；测评实施描述测评过程中涉及的具体测评方法以及需要实施的测评步骤；结果判定描述测评人员执行完测评实施过程、产生各种测评证据后，如何依据这些测评证据来判定被测系统是否满足测评指标的要求。

《测评要求》将等级测评分为单元测评和整体测评两部分，在保证相应安全等级的测评强度基础上，首先开展单元测评；在单元测评的基础上再开展整体测评。单元测评主要围绕如何对《基本要求》的每一项具体要求展开测评进行描述，包括采用什么测评方式对测评对象进行测评，测评后得到什么证据证明该项要求符合《基本要求》等，这些内容组成了《测评要求》的主体。在单元测评的基础上，对信息系统开展整体测评，可以进一步分析信息系统的整体安全性。整体测评主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。整体测评不但涉及信息系统的整体拓扑结构和局部设备部署，而且还关系到特定安全功能的实现和具体安全控制的配置。

《信息系统安全等级保护测评过程指南》（以下简称《测评过程指南》）为信息系

统安全等级测评工作建立了一套标准的测评过程，同时也对信息系统安全等级测评的工作任务、分析方法以及工作产品等提出了指导性的建议，以规范和指导信息系统安全等级测评工作，从而使得不同测评机构实施的信息系统安全等级测评过程、工作产品和测评结果更一致、更具有可比性、可重复性和可再现性。

等级测评是一项可以由不同测评机构实施的标准符合性测评工作。《测评过程指南》规定了开展该工作的基本过程、流程、任务及工作产品等，以规范测评机构的等级测评工作，与《测评要求》共同指导和规范等级测评工作。《测评过程指南》指导使用者如何开展等级测评，以及在等级测评过程中如何正确使用《测评要求》中的具体测评方法、步骤和判断依据等。

5.1.6 等级测评工作的开展

等级测评工作应按照“流程规范、方法科学、结论公正”的要求进行。

1．测评工作目标

按照《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》要求，各地区要在 2010 年底前完成 30%第三级以上信息系统的测评工作，2011 年底前完成所有第三级信息系统的测评工作。

2．测评工作内容

（1）制定工作计划，加强组织落实。各地区、各部门要按照公安部网络安全保卫局关于测评工作的整体部署，结合实际，制定本地区、本部门的测评工作计划，分解细化任务和目标，将长期目标和阶段性目标结合起来，明确具体要求，确定责任人员，加强组织领导，确保按期完成工作目标。各单位要根据工作计划并紧密结合本单位信息系统规模、数量、安全保护现状等实际情况，制定具体实施方案，明确进度安排、落实测评经费保障等，确保测评工作取得实效。

（2）委托符合要求的测评机构。各单位、各部门委托等级测评机构开展测评时，

应当在省级以上等保办公布的《测评机构推荐目录》中选择符合要求的测评机构。信息系统运营使用单位应当核查测评机构推荐证书、测评师证书等事项，约定合理的测评费用，并与测评机构签署委托测评合同。测评费用可以参考国家信息化项目人工计费标准或根据被测设备数量和测评项预算费用。测评机构应当结合实际编制测评作业指导书和测评实施方案，严格按照《信息安全等级保护测评工作管理规范》要求，规范开展测评工作，客观公正出具测评结论，并自觉接受监督。

（3）测评实施和方法。按照国家标准规范要求，测评实施过程包括测评准备、方案编制、现场测评以及分析与报告编制，等级测评的主要方法有：访谈、检查、测试、分析等。被测评信息系统运营使用单位与测评机构双方之间的沟通与洽谈，贯穿整个等级测评过程，为此信息系统运营使用单位应当指定专人协同配合，积极加强与测评机构间的协调沟通，确保测评进展顺利。

3．测评过程管理

在测评工作过程中，各单位、各部门要对测评活动进行监督管理，与测评机构签订工作协议和保密协议，落实测评过程监管措施，防范对信息系统可能造成新的安全风险。各单位、各部门要监督检查测评机构是否依据《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等国家标准开展等级测评，测评人员是否有违规行为。一旦发现违规行为，被测信息系统单位应当及时予以纠正，必要时可以向省级以上等保办反映。

4．测评报告的编写与备案

测评机构应当依据《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等标准规范开展等级测评，按照《信息系统安全等级测评报告模版》出具统一格式的测评报告，确保测评结论客观公正。各单位、各部门完成信息系统等级测评工作后 30 日内，将等级测评报告向受理备案的公安机关备案。公安机关应当对测评报告分析审核，建档留存，根据测评报告中的意见建议，督促指导备案单位及时开展安全建设整改工作。

5.2 等级测评机构及测评人员的管理与监督

5.2.1 为什么要开展等级测评体系建设工作

等级测评体系建设主要内容包括测评机构的建设和规范管理，测评人员和测评活动的规范管理等。信息安全等级保护测评工作是信息安全等级保护工作的重要环节，是专门机构针对信息系统开展的一种专业性、服务性的检测活动。等级测评工作涉及的信息系统范围广、敏感性强，参与的测评机构及测评人员复杂，如果缺乏对测评机构和测评人员的管理，则难以保证等级测评的客观、公正和安全，甚至会给重要信息系统安全造成新的风险和隐患，危害国家安全和社会稳定。为加强对测评机构及测评人员管理，稳步推进等级测评机构建设，规范等级测评活动，提高测评机构、人员的技术能力和水平，在国家信息安全等级保护协调小组的领导下，全国组织开展信息安全等级保护等级测评体系建设工作，以保障等级保护工作的顺利开展。

5.2.2 对测评机构和测评人员的管理

申请成为测评机构的单位（以下简称“申请单位”）可以向省级以上信息安全等级保护协调（领导）小组办公室提出申请，经过专门机构的能力评估和专门培训，对符合条件的申请单位，省级以上信息安全等级保护协调（领导）小组办公室推荐其成为等级测评机构，从事等级测评工作。省级信息安全等级保护协调（领导）小组办公室公布本地测评机构推荐目录，国家信息安全等级保护协调小组办公室公布《全国信息安全等级保护测评机构推荐目录》。

测评人员实行等级测评师管理。等级测评师分为初级、中级和高级。测评人员参加专门培训机构举办的专门培训和考试。考试合格的，由专门培训机构向测评人员颁发相应等级的《等级测评师证书》。《等级测评师证书》是测评人员上岗的基本

条件。

对测评机构等级测评师的要求是：从事第二级信息系统等级测评工作的测评机构至少应具有 6 名以上等级测评师，其中中级测评师不少于 2 名；第三级（含）以上信息系统等级测评工作的测评机构至少应具有 10 名以上等级测评师，其中中级测评师不少于 4 名，高级测评师不少于 2 名。

5.2.3 等级测评机构应当具备的基本条件

等级测评机构是指具备本规范的基本条件，经能力评估和审核，由省级以上信息安全等级保护工作协调（领导）小组办公室（以下简称为“等保办”）推荐，从事等级测评工作的机构。

等级测评机构应当具备以下基本条件。

（1）在中华人民共和国境内注册成立（港澳台地区除外）。

（2）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）。

（3）产权关系明晰，注册资金 100 万元以上。

（4）从事信息系统检测评估相关工作两年以上，无违法记录。

（5）工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

（6）具有满足等级测评工作的专业技术人员和管理人员，测评技术人员不少于 10 人。

（7）具备必要的办公环境、设备、设施，使用的技术装备、设施应当符合《信息安全等级保护管理办法》对信息安全产品的要求。

（8）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

（9）对国家安全、社会秩序、公共利益不构成威胁。

（10）应当具备的其他条件。

5.2.4 测评机构的业务范围和工作要求

1. 业务范围

测评机构除从事等级测评活动以外，还可以从事信息系统安全等级保护定级、等级保护安全建设整改、信息安全等级保护宣传教育等工作的技术支持，以及风险评估、信息安全培训、信息安全咨询和信息安全工程监理等工作。

2. 工作要求

从事等级测评工作的机构及其人员应当遵守国家有关法律法规，依据国家有关技术标准和本规范的相关规定，开展客观、公正、安全的测评服务，不得从事危害国家安全、社会秩序、公共利益以及被测单位利益的活动。

测评机构应当按照公安部统一制订的《信息系统安全等级测评报告模版》格式出具测评报告，根据信息系统规模和所投入的成本，合理收取测评服务费用。

5.2.5 测评机构的禁止行为

测评机构及其测评人员不得从事下列活动。

（1）影响被测评信息系统正常运行，危害被测评信息系统安全。

（2）泄露知悉的被测评单位及被测信息系统的国家秘密和工作秘密。

（3）故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具等级测评报告。

（4）未按规定格式出具等级测评报告。

（5）非授权占有、使用等级测评相关资料及数据文件。

（6）分包或转包等级测评项目。

（7）信息安全产品开发、销售和信息系统安全集成。

（8）限定被测评单位购买、使用其指定的信息安全产品。

（9）其他危害国家安全、社会秩序、公共利益以及被测单位利益的活动。

5.2.6 测评机构的申请、受理、审核、推荐流程

等级测评机构管理流程如图 5-1 所示。

1．测评机构的申请

知悉有关规定并愿意成为测评机构的申请单位，可以向省级以上等保办提出书面申请，如实填写《信息安全等级保护测评机构申请表》（见附录 J 的附件 1）。申请单位的人员应当如实填写人员基本情况表，并承诺对信息的真实性和有效性负责。

申请单位申请时，等保办应当告知测评机构的条件、从事的业务范围以及禁止行为等内容，使申请单位清楚了解测评机构的权利和义务。

2．受理申请

省级以上等保办负责等级测评机构的审核和推荐工作。国家信息安全等级保护工作协调小组办公室负责受理隶属国家信息安全职能部门和重点行业主管部门申请单位提出的申请。省级等保办负责受理本省（区、直辖市）申请单位提出的申请。

省级以上等保办对申请单位进行初审，初审通过的，应当告知申请单位到评估中心进行测评能力评估。

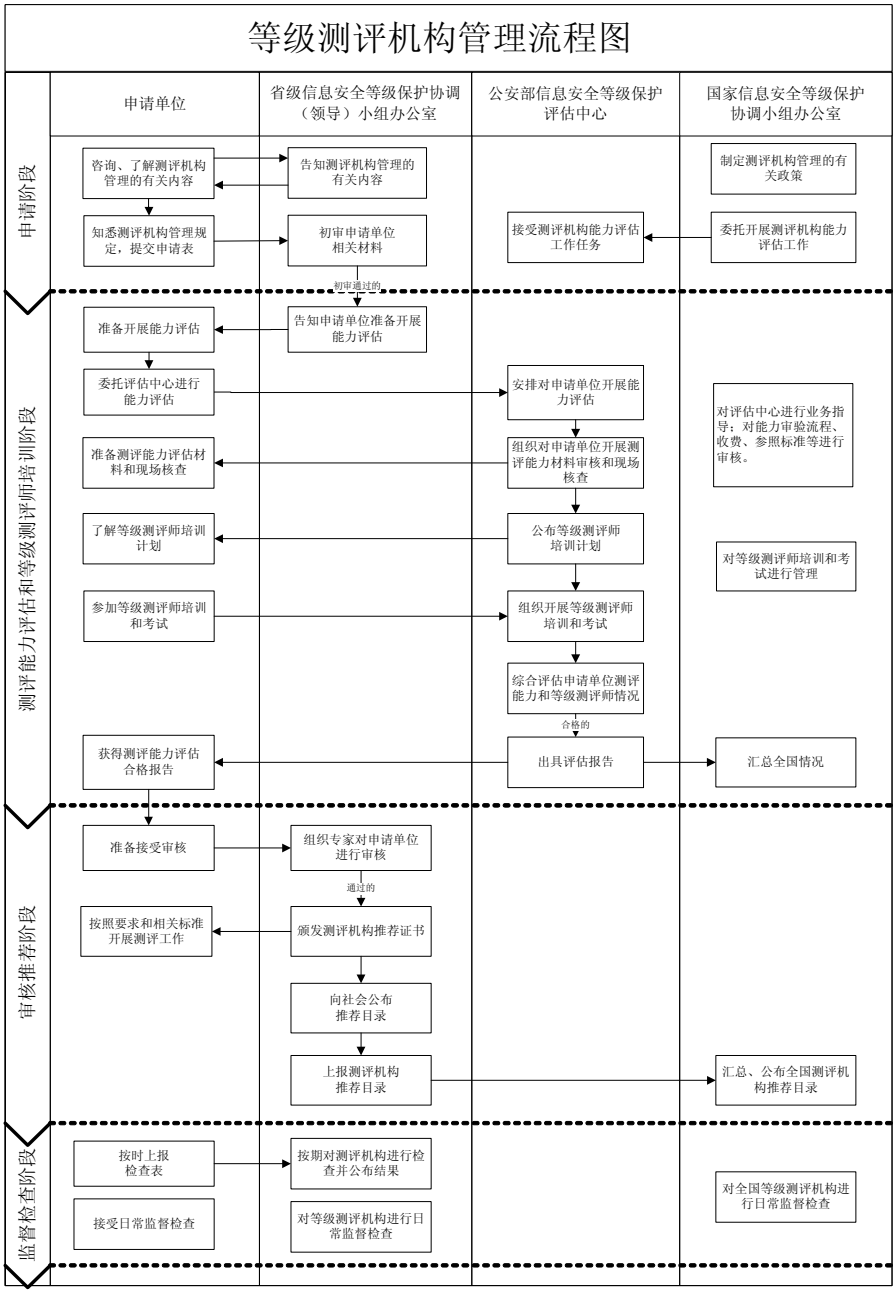

图 5-1　等级测评机构管理流程图

3．能力评估

公安部信息安全等级保护评估中心（以下简称“评估中心”）负责测评机构的能力评估和培训工作。评估中心按照有关标准规范，在 30 个工作日内完成对申请单位的材料审查和现场核查工作。

测评人员参加由评估中心举办的专门培训、考试并取得评估中心颁发的《等级测评师证书》（等级测评师分为初级、中级和高级）。等级测评人员需持等级测评师证上岗。

评估中心综合评估申请单位的测评能力，对测评能力评估合格的，出具评估报告。

4．审核和推荐

省级以上等保办组织专家对通过测评能力评估的申请单位及其测评人员进行审核。通过审核的，由省级以上等保办向申请单位颁发信息安全等级保护测评机构推荐证书（见附录 J 的附件 2），并向社会公布测评机构推荐目录。

省级等保办将测评机构推荐目录报国家信息安全等级保护工作协调小组办公室，国家信息安全等级保护工作协调小组办公室汇总公布《全国信息安全等级保护测评机构推荐目录》。

5.2.7　对测评机构的监督管理

1．定期检查

省级以上等保办每年对所推荐的测评机构进行检查，测评机构应提交《信息安全等级保护测评机构检查表》（见附录 J 的附件 3）。

2．变更

测评机构的名称、法人等事项发生变化，或者其等级测评师有变动，测评机构应在三十日内向受理申请的省级以上等保办办理变更手续。

3．申诉处理

测评机构应当严格遵循申诉、投诉及争议处理制度，妥善处理争议事件，及时采取纠正和改进措施。

4．违规处理

测评机构或者其测评人员违反 5.2.5 规定之一或年度检查未通过的，由省级以上等保办责令其限期改正；逾期不改正的，给予警告，直至取消测评机构的推荐证书或等级测评师证书，并向社会公告；造成严重损害的，由相关部门依照有关法律、法规予以处理。

测评机构或者测评人员违反《信息安全等级保护测评工作管理规范》的规定，给被测评单位造成损失的，应当依法承担民事责任。

5.3 等级测评的工作流程和工作内容

5.3.1 基本工作流程和工作方法

为确保等级测评工作的顺利开展，应首先了解等级测评的工作流程，以便对等级测评工作过程进行控制。等级测评基本工作流程如图 5-2 所示。

等级测评过程可以分为四个活动：测评准备、方案编制、现场测评以及分析与报告编制，而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。以下介绍等级测评流程中主要的工作内容，等级测评工作的完整内容参见标准《测评过程指南》。

等级测评的主要测评方法如下。

（1）访谈：访谈的对象主要是人员。

（2）检查：检查主要有评审、核查、审查、观察、研究和分析等。检查对象是文档、机制、设备等，工具是技术核查表。

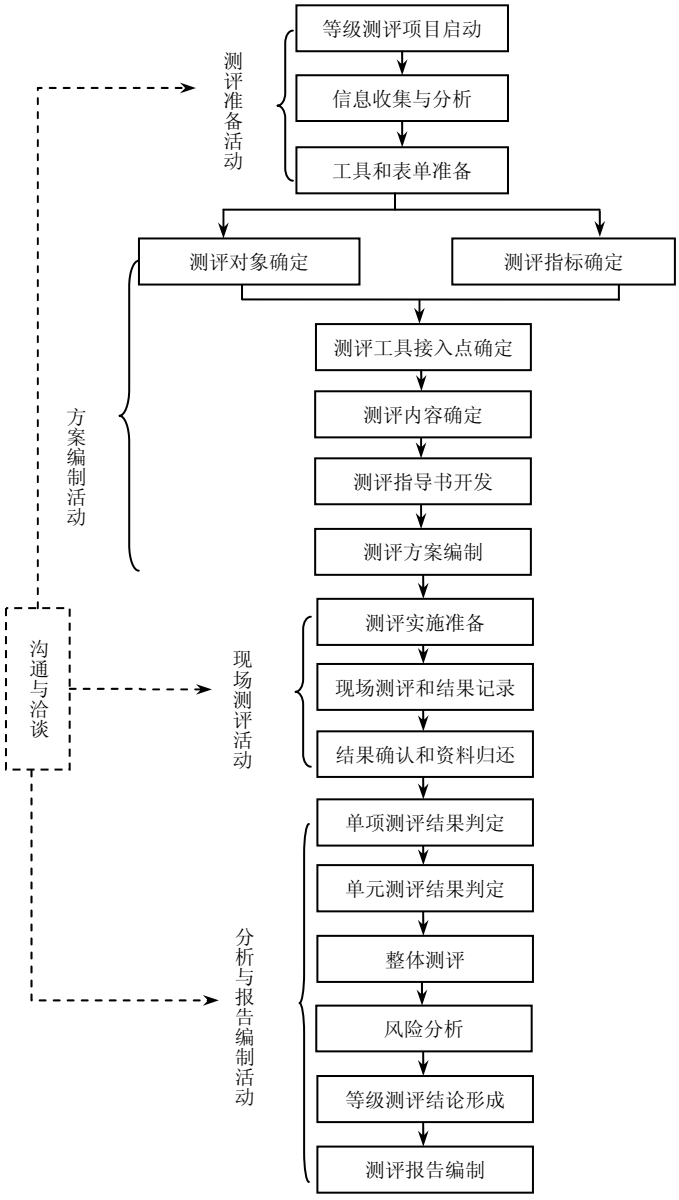

图 5-2　等级测评基本工作流程

（3）测试：主要是功能、性能测试及渗透测试，测评对象包括安全的机制，设

备等。

5.3.2 系统信息收集

与信息系统相关的信息收集是完成系统定级、等级测评、需求分析、安全设计等工作的前提，通常收集信息的方法是以发放调查表格的形式，通过与人员访谈、资料查阅、实地考察等方式完成。

与信息系统相关的信息包括物理环境信息、网络信息、主机信息、应用信息和管理信息等，以下简要介绍信息系统相关信息的收集方法。

1．物理环境信息收集

信息系统所在物理环境的信息收集包括机房数量、每个机房中部署的信息系统、机房物理位置、办公环境的物理位置等。

2．系统网络信息收集

信息系统网络信息的收集涉及网络拓扑图、网络结构情况、系统外联情况、网络设备情况和安全设备情况等。

（1）网络拓扑图

应获得信息系统最新的网络拓扑图，并保证网络拓扑图清晰地标示出网络功能区域划分、网络与外部的连接、网络设备、服务器设备和主要终端设备等情况。最新的网络拓扑图可以了解整个信息系统的网络结构，同时也是与被测系统网络管理人员沟通的基础。

（2）网络结构情况

网络结构的信息收集内容包括网络功能区域划分情况、各个区域的主要功能和作用、每个网络区域的 IP 网段地址、每个区域中的服务器和终端数量、与每个区域相连的其他网络区域、网络区域之间的互联设备、每个区域的重要程度等。

（3）系统外联情况

由于信息系统的出口（即信息系统的外联情况）是与外界直接相连的，面临的威胁较多，因此是信息收集过程中重要的关注环节。系统外联的信息收集内容包括外联单位的名称、外联线路连接的网络区域、接入线路的种类、线路的传输速率（带宽）、外联线路的接入设备以及外联线路上承载的主要业务应用等。

（4）网络设备情况

网络设备的信息收集内容包括网络设备名称、设备型号、设备的物理位置、设备所在的网络区域、设备的 IP 地址/掩码/网关、设备的系统软件、软件版本及补丁情况、设备端口类型及数量、设备的主要用途、是否采用双机热备等。设备型号及系统软件相关情况是选择或开发测评指导书的基础，设备的 IP 地址等情况是接入测试工具所必须了解的。设备的主要用途则是选择测评对象时需要考虑的。

（5）安全设备情况

安全设备包括防火墙、网关、网闸、IDS、IPS 等。安全设备的信息收集内容包括安全设备名称、设备型号、设备是由纯软件还是由软硬结合件构成、设备的物理位置、设备所在的网络区域、设备 IP 地址/掩码/网关、设备上的系统软件及运行平台、设备的端口类型及数量、是否采用双机热备等。设备型号及系统软件相关情况是选择或开发测评指导书的基础。

3．主机信息收集

信息系统主机信息的收集涉及服务器设备情况和终端设备情况等。

（1）服务器设备情况

服务器设备的信息收集内容包括服务器设备名称、型号、物理位置、所在的网络区域、IP 地址/掩码/网关、安装的操作系统版本/补丁、安装的数据库系统版本/补丁、服务器承载的主要业务应用、服务器安装的应用系统软件、服务器中应用涉及的业务数据、服务器的重要程度、是否采用双机热备等。服务器型号、操作系统及数据库系

统情况是选择或开发测评指导书的基础。服务器承载的主要业务应用可以了解业务应用与设备的关联关系，服务器的重要程度则是选择测评对象时的考虑因素之一。

（2）终端设备情况

终端设备的信息收集对象一般包括业务终端、管理终端、设备控制台等。终端设备的信息收集内容包括终端设备名称、型号、物理位置、所在的网络区域、IP 地址/掩码/网关、安装的操作系统/补丁、安装的应用系统软件名称、涉及的业务数据、终端的主要用途、终端的重要程度、同类终端设备的数量等。

4．应用信息收集

信息系统应用信息的收集涉及应用系统情况和业务数据情况等。

（1）应用系统情况

业务应用系统的信息收集内容包括业务（服务）的名称、业务的主要功能、业务处理的数据、业务应用的用户数量、用户分布范围、业务采用的应用系统软件名称、应用系统的开发商、应用系统采用 C/S 或 B/S 模式、业务应用是否 24 小时运行、业务的重要程度、应用软件的处理流程等。

（2）业务数据情况

业务数据的信息收集内容包括业务数据名称、涉及的业务应用、数据总量及日增量、数据存放所在的服务器、是否有单独的存储系统、数据的备份周期、数据是否异地保存、数据的重要程度等。

5．管理信息收集

管理信息的收集内容包括管理机构的设置情况、人员职责的分配情况、各类管理制度的名称、各类设计方案的名称等。管理机构的设置情况和人员职责的分配情况主要通过一些开放性问题进行访谈交流的方式获取。

5.3.3 编制测评方案

在测评工作中，编制好测评方案是相当重要的，一方面测评方案是测评人员进行内部工作交流、明确工作任务的指南，另一方面，测评方案给出具体的现场测评工作思路、方式、方法和具体测评对象及内容，为现场测评的顺利完成打下基础；此外，通过测评方案，可以和被测系统运营使用单位进行充分的交流，让被测系统运营使用单位理解并支持现场测评工作，并依据测评方案做好充分的准备。因此，可以说测评方案的好坏在很大程度上决定着一次测评工作能否顺利完成。

测评方案应包括但不局限于以下内容：项目概述、工作依据、测评计划、被测系统描述、测评指标说明、测评对象说明、测评内容和方法等。其中，几个关键部分说明如下。

1．测评方案的基本内容

（1）被测系统描述

本部分描述被测系统的情况。需要根据被测系统定级情况，确定被测系统的范围，包括整个信息系统的范围、被测系统的范围及边界等。

对被测系统进行描述时，一般以信息系统的网络拓扑结构为基础，采用总分式的描述方法，先说明被测系统的整体结构，然后描述被测系统的边界，最后介绍被测系统的网络区域及具体主机设备节点等。

被测系统的整体结构描述，应包括被测系统的标识（名称）、被测系统的物理环境、被测系统的网络拓扑结构和被测系统的外部边界连接情况等，并给出网络拓扑图。

被测系统的边界描述，应包括被测系统与其他网络进行外部连接的边界连接方式，如采用光纤、无线和专线等；描述各边界主要设备，如防火墙、路由器或服务器等。如果在信息系统边界连接处有共用设备，一般可以把该设备划到等级较高的

那个信息系统中。

（2）测评计划

本部分描述现场工作人员的分工和计划。进行现场测评人员分工和时间计划安排时，需要先确定工作量以及工作人员数量，然后再根据工作量和人员数量等情况进行具体的安排。工作量的确定可以根据配置检查的节点数量和工具测试的接入点及测试内容等情况进行估算。另一方面，需要注意的是，在进行时间计划安排时，应尽量避开信息系统的业务高峰期，避免给被测系统带来影响。

可以根据需要进行配置检查的网络设备和主机设备数量，以及工具测试的接入点和测试内容等情况预估现场测评工作量。一般对一台主机设备进行配置检查，需要一个小时左右。在百兆网络环境下，在一个接入点，扫描一台主机设备需要半个小时左右。

（3）测评指标

本部分描述对被测系统进行测评的测评指标，可以以列表的形式给出。测评指标应该根据被测系统的级别确定，关于测评指标的选择在后面介绍。

（4）测评对象

本部分描述选取的测评对象情况，可以采用列表的方式进行描述。测评对象是等级测评的一项重要工作，关于测评对象的选择在后面介绍。

（5）现场测评实施内容

本部分描述实施现场测评的具体实施内容。等级测评包括两个方面：单元测评和整体测评，因此，现场测评实施内容也主要从这两个方面分别展开。确定单元测评内容首先要依据《测评要求》，将上述几个步骤得到的测评指标、测评方式以及测评对象结合起来，然后再将测评对象与具体的测评方法和步骤结合起来，这也是编制测评指导书的第一步。整体测评内容主要是依据《测评要求》中的整体测评方法，结合信息系统的实际情况，根据现场测评的结果记录进行分析。

2．测评指标和测评对象的选择方法

在编制测评方案时，测评指标的选择和测评对象的选择是一项比较重要的工作，以下简要介绍选择方法。

（1）测评指标确定方法

《基本要求》是等级测评依据的主要标准。在等级测评时，这些基本要求可以转化为针对不同被测系统的测评指标。

由于信息系统不但有安全保护等级，还有业务信息安全保护等级和系统服务安全保护等级，而《基本要求》中的各项要求也分为业务信息安全保护类、系统服务安全保护类和通用安全保护类要求，从而测评指标也应该由这三类组成。

确定测评指标的具体步骤如下。

① 根据调查结果得到被测系统的安全保护等级、业务信息安全保护等级和系统服务安全保护等级。

② 从《基本要求》中选择与被测系统的安全保护等级对应的保护要求类别为“G类”的所有基本要求。

③ 从《基本要求》中选择与被测系统的业务信息安全保护等级对应的保护要求类别为“S 类”的所有基本要求。

④ 从《基本要求》中选择与被测系统的系统服务安全保护等级对应的保护要求类别为“A 类”的所有基本要求。

⑤ 如果同时测评的多个被测系统位于同一个物理环境中，而且有的管理方面采用相同的管理，则采取就高原则，选择所有被测系统中最高级别的物理安全和相同管理方面对应的基本要求作为物理安全和一些管理安全方面的测评指标。

⑥ 综合 1～5 步得到的基本要求作为被测系统的测评指标。

举例来说，假设某信息系统的定级结果为：系统安全保护等级为三级，业务信

息安全保护等级为二级，系统服务安全保护等级为三级，则该系统的测评指标将包括《基本要求》“技术要求”中的三级通用指标类（G3），二级业务信息安全性指标类（S2），三级业务服务保证性指标类（A3），以及第三级“管理要求”中的所有指标类。如果同时测评的另外一个信息系统的定级结果为：系统安全保护等级为四级，业务信息安全保护等级为四级，系统服务安全保护等级为三级，而且这两个信息系统共用机房，由相同的人员进行管理，所有的管理内容都采用相同的管理方法，则应调整物理安全的测评指标为四级通用指标类（G4），四级业务信息安全性指标类（S3），三级业务服务保证性指标类（A3），调整管理安全测评指标为四级“管理要求”中的所有指标类。

（2）测评对象确定方法

测评对象是等级测评的直接工作对象，也是在被测系统中实现特定测评指标所对应的安全功能的具体系统组件，因此，选择测评对象是测评的必要步骤，也是整个测评工作的重要环节。恰当选择测评对象的种类和数量是整个等级测评工作能够获取足够证据、了解到被测系统的真实安全保护状况，也是实现不同等级信息系统测评强度要求的重要保证。

测评对象的选择一般采用抽查方式，即：抽查信息系统中具有代表性的组件作为测评对象。抽查的对象可以多也可以少，比较灵活。但是，测评对象选择的过多会导致测评工作量投入过多、花费过大；过少则会导致不能保证达到相应等级信息系统的测评强度要求，测评结果不够充分、可信，不能够真实地反映信息系统是否达到相应等级的安全保护要求，具有相应的安全保护能力。因此，在测评对象选择过程中应兼顾工作投入和结果产出两者的平衡关系，尽量抽查有代表性的组件（根据安全需求分析的结果，各层面实现主要安全要求、对系统安全保护能力起决定作用的组件）作为测评对象。

不同等级的信息系统进行等级测评时，选择的测评对象的数量和种类应该不同，随着信息系统安全等级的增加，抽查的测评对象的种类和数量也应该随之增加。针对不同等级的信息系统采用规定的方式确定测评对象的种类，即规定哪种类型的测

评对象是必查的，哪些测评对象的种类是选查的；而对于同一种类并且在整个信息系统中作用相同或相近的测评对象采用抽样的方式确定其数量，如某一种业务应用的安全终端、不同楼层的楼层交换机如果有多台，可以采用抽样的方式分别确定选择哪几台作为测评对象。针对不同等级安全测评，测评对象的抽查种类和数量，应该能够承担相应等级所有的安全要求，应该能够满足相应等级系统整体测评中区域间测评的需要，应该能够保证相应等级的测试工作量投入。

5.3.4 现场测评

现场测评活动全部在被测系统现场完成，需要测评机构、测评委托单位（若测评委托单位与被测系统运营、使用单位不同的，还应有被测系统运营、使用单位）的全程参与。整个活动过程中，测评机构应与对方充分沟通和协调，以便顺利完成测评任务。另外，测评人员测评过程中应不直接接触被测系统，由对方配合人员进行操作，测评人员只负责查看、获取以及详细、准确、规范记录测评证据，并保留电子证据，以便为后期的结果分析和报告编制准备充足、翔实的资料。

现场安全测评涉及的基本手段是访谈、检查和测试。访谈是测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一种方法。

信息系统级别不同，现场安全测评采用的手段和测评的强度也不同，以下以网络安全为例，说明现场安全测评可能关注的内容和采用的方法。

1．一级信息系统网络安全测评

对于一级信息系统，主要使用访谈和检查两种测评方式。在访谈方面，只要求对网络管理员和安全员进行简单扼要的访谈；在检查方面，重点查看边界和关键网

络设备安全方面采取了哪些具体措施。访谈和检查测评覆盖结构安全、访问控制和网络设备防护等三个测评单元。

（1）对于“结构安全”，重点询问关键网络设备的业务处理能力、网络接入及核心网络的带宽是否满足业务需要；主要检查网络拓扑图，查看其与当前运行的实际网络系统是否一致。对一级信息系统，能检查到网络拓扑图与当前运行情况一致，访谈说明关键网络设备的处理能力满足基本业务需求，网络接入及核心网络的带宽满足业务需要，就大致可以判断系统满足一级“结构安全与网段划分”的要求。

（2）对于“访问控制”，重点询问采取哪些网络访问控制措施，网络访问控制设备具备哪些访问控制功能；主要检查边界网络设备（包括网络安全设备）有无正确的访问控制列表。对一级信息系统，能检查到边界网络设备（包括网络安全设备）有正确的访问控制列表对数据的源地址、目的地址、源端口、目的端口、协议等进行控制，就大致可以判断系统满足一级“网络访问控制”的要求。

（3）对于“网络设备防护”，重点询问对关键网络设备采取哪些防护措施，对其登录做过何种特定安全配置；主要检查边界和关键网络设备的安全配置有无对登录其的用户进行限制，有无对鉴别失败采取锁定措施，有无配置对设备远程管理所产生的鉴别信息进行保护的功能等。对一级信息系统，能检查到边界和关键网络设备的安全配置对登录其的用户有无身份鉴别，并限制非法登录次数，多次登录失败后锁定账号，有鉴别信息保护功能等，就大致可以判断系统满足一级“网络设备防护”的要求。

2．二级信息系统网络安全测评

对二级信息系统，主要是在一级的测评基础上，增加了一些访谈细节、功能测试、渗透测试方面的测评要求。主要测评方式除访谈和检查以外增加了测试。在检查对象方面，增加了网络设计/验收文档等，并增加了安全审计、边界完整性检查和入侵防范等三个测评单元，扩大了测评范围，并对重要网络设备进行关注。

（1）对于“结构安全”，二级信息系统在一级信息系统的测评基础上，增加了询

问网段划分情况、带宽控制情况和分配原则；增加检查网络设计和验收文档中有无关于子网或网段划分及其地址分配情况的说明。通过了解网络拓扑结构、网络设计/验收文档、网段划分、地址分配以及边界和重要网络设备的安全配置情况，从而确定其是否达到二级要求。

（2）对于“访问控制”，二级信息系统在一级信息系统的测评基础上，访谈增加询问访问控制策略的设计原则，是否允许拨号访问网络，增加检查边界网络设备有无根据会话状态信息对数据流进行控制，是否限制具有拨号访问权限的用户数量，增加了测试边界网络设备有无对未授权的访问行为采取控制措施。通过了解边界网络设备采取的网络访问控制措施，从而确定其是否达到二级要求。

（3）对于“网络设备防护”，二级信息系统在一级信息系统的测评基础上，访谈增加询问网络设备的口令策略，增加检查身份鉴别信息的复杂性和定期修改要求，有无对管理员登录地址进行限制；增加了渗透性测试边界和重要网络设备的配置情况。通过了解边界和重要网络设备的安全配置情况，从而确定其是否达到二级要求。

3．三级信息系统网络安全测评

对三级信息系统，主要是在二级的测评基础上，增加了一些细节和渗透测试等方面的测评要求。主要测评方式包括访谈、检查和测试三种，对主要网络设备进行关注，扩大了测评范围。

（1）对于“结构安全”，在二级信息系统测评的基础上，三级信息系统增加访谈询问网段具体的部署位置、与其他网段的隔离措施等，增加询问网络管理员网络设备的路由控制策略、策略设计的目的等内容，增加检查边界和主要网络设备的路由控制策略、网段隔离措施、带宽控制策略等。通过了解网络拓扑结构、网段划分、地址分配、带宽策略以及边界和主要网络设备的安全配置情况，从而确定其是否达到三级要求。

（2）对于“访问控制”，在二级信息系统测评的基础上，三级信息系统增加检查边界网络设备对数据流的控制是否为端口级，边界网络设备有无对进出网络的信息内容进行过滤，有无对网络接入、终止连接、网络最大流量数及网络连接数进行限

制，网络地址与数据链路地址绑定，防止内部网络信息外泄措施等；增加了测试验证主要网络设备访问控制力度，增加了对网络访问控制措施进行渗透测试。通过了解边界和主要网络设备采取的访问控制措施以及渗透测试对其有效性的验证，从而确定其是否达到三级要求。

（3）对于“网络设备防护”，在二级信息系统测评的基础上，三级信息系统访谈增加网络特权用户的权限分配原则，检查增加边界和主要网络设备上的安全配置有无对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，检查是否设置网络登录连接超时自动退出、特权用户的权限分离等措施。通过了解边界和主要网络设备的防护能力，从而确定其是否达到三级要求。

4．四级信息系统网络安全测评

对四级信息系统，主要是在三级的测评基础上，部分控制点增加了一些检查和渗透测试等方面的测评要求。主要测评方式包括访谈、检查和测试三种，对所有网络设备进行关注，扩大了测评范围。

（1）对于“访问控制”，在三级信息系统测评的基础上，四级信息系统主要是限制网络接入等，询问有无对网络访问控制策略进行过调整；检查是否禁止数据带通用协议通过，禁用远程拨号访问功能，增加检查网络设计/验收文档内容，并增加了渗透性测试内容，验证访问控制措施是否有效阻断带通用协议的数据。通过了解边界和主要网络设备采取的访问控制措施以及渗透测试对其有效性的验证，从而确定其是否达到四级要求。

（2）对于“网络设备防护”，在三级信息系统测评的基础上，四级信息系统增加了身份鉴别技术的强度。

5.3.5 测评结果判断

在对每个测评对象实施现场测评时，一般是按照测评项一条一条分别进行测评的。根据不同的测评方式、测评内容等，执行现场测评后，会得到多个测评证据。

这就可能会出现多个测评证据存在矛盾的情况，即有的测评证据与其预期结果一致，有的测评证据与其预期结果不一致。在这种情况下，如何根据这些不一致的测评证据给出单个测评项的测评结果呢？测评结果判断通常分为单项结果判定和单元结果判定两类。

1．单项结果判定

（1）单个测评项说明

单个测评项对应《基本要求》中的要求项。对于单个测评项的具体内容分为两种情况：① 每个要求项只提出一方面的要求内容，如“应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；”；② 每个要求项含有两个或多个方面的要求内容，如“安全管理制度应注明发布范围，并对收发文进行登记。”这个要求项就包含“安全管理制度应注明发布范围”和“对收发文进行登记”两个方面的要求内容。

（2）单项测评结果判定

单项测评结果的形成通常分为三步。

① 针对每个测评项，分析该测评项所对抗的威胁在被测系统中是否存在，如果不存在，则该测评项应标为不适用项。

② 分析单个测评项是否有多方面的要求内容，依据“优势证据”法针对每一方面的要求内容，从一个或多个测评证据中选择出“优势证据”，并将“优势证据”与要求内容的预期测评结果相比较。

③ 如果测评证据表明所有要求内容与预期测评结果一致，则判定该测评项的单项测评结果为符合；如果测评证据表明所有要求内容与预期测评结果不一致，判定该测评项的单项测评结果为不符合；否则判定该测评项的单项测评结果为部分符合。

（3）“优势证据”法

在判断单个测评项的某个要求小项的测评结果时，可能会出现两种情况：情况

一，多个测评证据与预期测评结果都相符合或者都不符合；情况二，在多个测评证据中，其中一些测评证据与预期结果不符，而另外一些测评证据则与预期结果相符，也就是说，多个测评证据之间出现“矛盾”。对于情况一，是一种比较理想的情况，多个测评证据都符合或者都不符合，自然该要求小项的测评结果为：符合或者不符合。但对于情况二，要求小项的测评结果就很难确定。

为解决情况二中所产生的测评证据“矛盾”的问题，引用在法学中的“优势证据”原则。在民事诉讼中，当双方当事人对同一事实分别举出相反证据，但都没有足够的证据否定对方证据的，法院应结合案件情况，判断一方提供的证据的证明力是否明显大于另一方提供证据的证明力，并对证明力较大的证据予以确认。这就是“优势证据”确立的原因。在单个要求小项的测评结果判定的过程中，也遇到了类似的问题，因此，采用“优势证据”不失为解决问题的一个方法。

所谓“优势证据”，是指在得到的多个测评证据中那个/些对于单个要求小项的符合性判定更具有证明力、说服力的测评证据。由于不同测评人员对优势证据的理解可能不同，即选择的优势测评证据就不同，测评结果可能会因此而不同。为避免这种情况出现，需使用“优势证据”法。具体从测评方式上来讲，针对技术安全方面的测评来说，单个要求小项的结果判定时的优势证据顺序一般为：配置检查证据>工具测试证据>访谈证据；对于物理安全测评来说，优势证据顺序一般为：实地察看证据>文档审查证据>访谈证据；对于管理安全方面的测评来说，则要根据实际情况分析确定优势证据。

2．单元测评结果判定

单元测评结果的判定涉及该单元测评实施的测评对象和测评项。一般来说，一个测评单元可能在多个测评对象上实施，而且一个测评单元往往包含多个测评项。因此，如何在单一测评对象的单一测评项的测评结果基础上形成针对单个测评对象和多个测评项的单元测评的结果是单元测评结果判定方法的核心。

单元测评结果是在单项测评结果基础上汇总得到的，判定原则为：

① 单元测评指标包含的所有测评项均为不适用项，则该测评对象对应该测评指

标的单元测评结果为不适用。

② 单元测评指标包含的所有测评项的单项测评结果均为符合或不符合，则该测评对象对应该测评指标的单元测评结果为符合或不符合。

③ 单元测评指标包含的所有测评项的单项测评结果不全部为符合或不符合或不适用，则该测评对象对应该测评指标的单元测评结果为部分符合。

单元测评结果一般通过分层面、分测评对象统计不同安全控制的不同测评对象的单项测评结果得到，并以表格的形式逐一列出。单元测评结果一方面可以以一览表形式给出单元测评结果，另一方面，它也是整体测评中安全控制间、层面间和区域间测评分析的基础。单项测评判定结果、单元测评判定结果以及各种汇总表说明见 5.5 节“等级测评报告的主要内容”。

5.3.6 测评报告编制

测评报告是等级测评工作的最终产品，直接体现测评的成果。而且，测评报告编制不好，不但不能很好地反映测评机构的能力，还可能引发不必要的争议。应按照公安部的统一格式要求出具信息系统等级测评报告。

测评报告应包括以下内容：报告摘要、测评项目概述、被测信息系统情况、等级测评范围与方法、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、安全建设整改建议等。具体内容说明见 5.5 节“等级测评报告的主要内容”。

5.4 等级测评工作中的风险控制

5.4.1 存在的风险

等级测评过程中可能存在以下风险。

1. 信息系统敏感信息泄漏

泄漏被检测单位信息系统状态信息，如网络拓扑、IP 地址、业务流程、安全机

制、安全隐患和有关文档信息。

2．验证测试对运行系统可能会造成影响

在现场测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机查看一些信息，这就可能对系统的运行造成一定的影响，甚至存在误操作的可能。

3．工具测试对运行系统可能会造成影响

在现场测评时，会使用一些技术测试工具进行漏洞扫描测试、性能测试甚至抗渗透能力测试。测试可能会对系统的负载造成一定的影响，漏洞扫描测试和渗透测试可能对服务器和网络通信造成一定影响甚至伤害。

5.4.2 风险的规避

在等级测评过程中可以通过采取以下措施规避风险。

1．签署保密协议

测评双方应签署完善的、合乎法律规范的保密协议，以约束测评双方现在及将来的行为。保密协议规定了测评双方保密方面的权利与义务。测评工作的成果属被测系统运营、使用单位所有，测评机构对其的引用与公开应得到被测系统运营、使用单位的授权，否则被测系统运营、使用单位将按照保密协议的要求追究测评机构的法律责任。

2．签署委托测评协议

在测评工作正式开始之前，测评方和被测系统运营、使用单位需要以委托测评协议的方式明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等。使得测评双方对测评过程中的基本问题达成共识，后续的工作以此为基础，避免以后的工作出现大的分歧。

3．现场测评工作风险的规避

进行验证测试和工具测试时，测评机构需要与测评委托单位充分的协调，安排好测试时间，尽量避开业务高峰期，在系统资源处于空闲状态时进行，并需要被测系统运营、使用单位对整个测试过程进行监督；在进行验证测试和工具测试前，需要对关键数据做好备份工作，并对可能出现的影响制定相应的处理方案；上机验证测试原则上由被测系统运营、使用单位相应的技术人员进行操作，测评人员根据情况提出需要操作的内容，并进行查看和验证，避免由于测评人员对某些专用设备不熟悉造成误操作；测评机构使用的测试工具在使用前应事先告知被测系统运营、使用单位，并详细介绍这些工具的用途以及可能对信息系统造成的影响，征得其同意。

4．规范化的实施过程

为保证按计划、高质量地完成测评工作，应当明确测评记录和测评报告要求，明确测评过程中每一阶段需要产生的相关文档，使测评有章可循。在委托测评协议、现场测评授权书和测评方案中，需要明确双方的人员职责、测评对象、时间计划、测评内容要求等。

5．沟通与交流

为避免测评工作中可能出现的争议，在测评开始前与测评过程中，双方需要进行积极有效的沟通和交流，及时解决测评中出现的问题，这对保证测评的过程质量和结果质量有重要的作用。

5.5 等级测评报告的主要内容

5.5.1 等级测评报告的构成

信息系统的运行使用单位选择测评机构完成等级测评工作后，应要求等级测评机构按照公安部制定的《信息系统安全等级测评报告模版（试行）》出具等级测评报

告。等级测评报告是等级测评工作的最终产品，直接体现测评的成果。按照公安部对等级测评报告的格式要求，测评报告应包括但不局限于以下内容：报告摘要、测评项目概述、被测信息系统情况、等级测评范围与方法、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、安全建设整改建议等。

5.5.2 等级测评报告的主要内容说明

1．测评项目概述

描述本次测评的主要测评目的和依据、测评过程、报告分发范围。

2．被测信息系统情况

简要描述本次测评的被测系统情况，包括承载的业务情况、网络结构、系统构成情况（包括业务应用软件、关键数据类别、主机/存储设备、网络互联设备、安全设备、安全相关人员、安全管理文档、安全环境等）、前一次测评发现的主要问题和测评结论等。

3．等级测评范围与方法

描述本次测评的测评指标、测评对象选择方法及选中的测评对象、测评过程中用到的测评方法等。

4．单元测评

主要是针对测评指标，结合测评对象（网络设备、主机和业务应用系统等），分层面描述单元测评指标的符合情况，包括现场测评中获取的测评证据记录、结果汇总以及发现的问题分析等。

5．整体测评

针对单项测评结果的不符合项，从安全控制间、层面间、区域间和系统结构等方面对单元测评的结果进行验证、分析和整体评价。

6．测评结果汇总

以不同的表现形式汇总测评结果，包括单元测评结果汇总、不同设备和安全子类的测评结果汇总、安全问题汇总等。

7．风险分析和评价

风险分析和评价主要针对测评汇总结果中的安全问题进行风险分析和评价，给出可能的风险等级。风险等级分为高、中、低三级。这里要求的风险分析和评价不是指对整个信息系统再进行一次风险评估工作，只是要求针对等级测评中发现的安全问题，分析判断安全问题导致安全事件可能对信息安全性和服务连续性造成的最大影响，以及安全问题导致安全事件发生的可能性，给出安全问题的风险。风险分析和评价主要根据汇总整理出的安全问题，用表格的形式给出每个安全问题可能的风险。

8．等级测评结论和整改建议

综合上述的分析，给出等级测评结论和安全建设整改建议。

等级测评结论章节主要给出被测评信息系统的等级测评结论，信息系统等级测评结论分为符合、基本符合和不符合。如果等级测评过程中没有发现安全问题，全部测评项均为符合，则等级测评结论为符合，否则应为基本符合或不符合。

目前，给出等级测评结论为基本符合或不符合的依据是风险分析和评价结果。对等级测评中发现的安全问题进行风险分析和评价，给出可能的风险等级，风险等级分为高、中、低三级，如果没有风险等级为“高”的安全问题，则等级测评结论为基本符合，否则为不符合。

等级测评过程和测评结论的产生如图 5-3 所示。

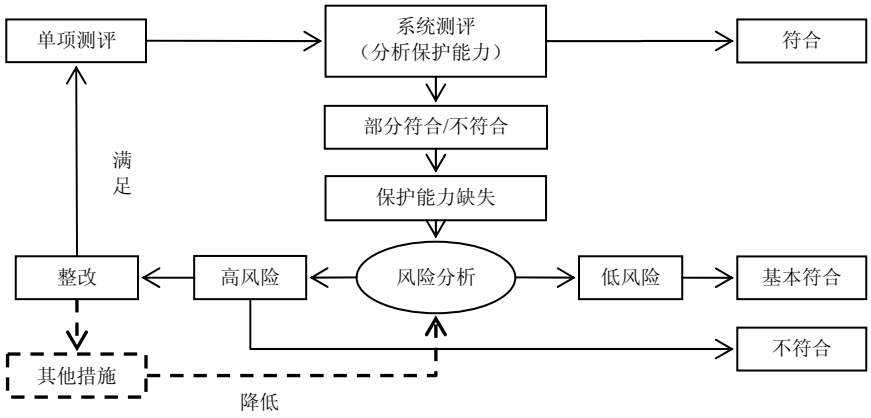

图 5-3　等级测评过程和测评结论的产生

某项要求没有实现并不一定意味着不符合基本要求，需要分析系统是否有能力对抗相关威胁、分析安全目标是否达到。某一层面安全要求不能达到，可以通过有互补关系的其他层面的安全措施来弥补，减少相应风险。

CHAPTER

6

第 6 章　安全自查和监督检查

备案单位、行业主管部门、公安机关要分别建立并落实监督检查机制，定期对等级保护制度各项要求的落实情况进行自查和监督检查。

6.1　定期自查与督导检查

6.1.1　备案单位的定期自查

备案单位应按照《管理办法》的相关要求，对等级保护工作落实情况进行自查，掌握信息系统安全状况、安全管理制度及技术保护措施的落实情况等，及时发现安全隐患和存在的突出问题，有针对性地采取技术和管理措施。第三级信息系统是否每年进行一次自查，第四级信息系统是否每半年进行一次自查。经自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位进一步进行安全建设的整改。

备案单位应当配合公安机关的监督检查工作，如实提供有关资料及文件。当第三级（含）以上信息系统发生事件、案件时，备案单位应当及时向受理备案的公安机关报告。

6.1.2 行业主管部门的督导检查

行业主管部门要建立督导检查制度，组织制定本行业、本部门的信息安全等级保护检查工作规范，定期组织对本行业、本部门等级保护工作开展情况进行检查，督促落实信息安全等级保护制度，达到重点督促、以点带面的目的。

6.2 公安机关的监督检查

6.2.1 检查的原则和方法

公安机关信息安全等级保护检查工作是指公安机关依据有关规定，会同主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，督促、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员。

部、省、市三级公安机关网络安全保卫部门依据《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736 号），定期对备案单位等级保护工作开展和实施情况进行监督检查。每年对第三级信息系统的运营使用单位信息安全等级保护工作检查一次，每半年对第四级信息系统的运营使用单位信息安全等级保护工作检查一次。信息安全等级保护检查工作采取询问情况，查阅、核对材料，调看记录、资料，现场查验等方式进行。

6.2.2 检查的主要内容

检查的主要内容包括：① 等级保护工作组织开展、实施情况。安全责任落实情况，信息系统安全岗位和安全管理人员设置情况；② 按照信息安全法律法规、标准规范的要求制定具体实施方案和落实情况；③ 信息系统定级备案情况，信息系统变化及定级备案变动情况；④ 信息安全设施建设情况和信息安全整改情况；⑤ 信息

安全管理制度建设和落实情况；⑥ 信息安全保护技术措施建设和落实情况；⑦ 选择使用信息安全产品情况；⑧ 聘请测评机构按规范要求开展技术测评工作情况，根据测评结果开展整改情况；⑨ 自行定期开展自查情况；⑩ 开展信息安全知识和技能培训情况。

有关具体检查项目见附录 E《公安机关信息安全等级保护检查工作规范（试行）》。

6.2.3 检查整改要求

检查时，发现不符合信息安全等级保护有关管理规范和技术标准要求，具有下列情形之一的，应当通知其运营使用单位限期整改，并发送《信息系统安全等级保护限期整改通知书》。逾期不改正的，给予警告，并向其上级主管部门通报以下情况：

① 未按照《管理办法》开展信息系统定级工作的；② 信息系统安全保护等级定级不准确的；③ 未按《管理办法》规定备案的；④ 备案材料与备案单位、备案系统不符合的；⑤ 未按要求及时提交《信息系统安全等级保护备案表》表四的有关内容的；⑥ 系统发生变化，安全保护等级未及时进行调整并重新备案的；⑦ 未按《管理办法》规定落实安全管理制度、技术措施的；⑧ 未按《管理办法》规定开展安全建设整改和安全技术测评的；⑨ 未按《管理办法》规定选择使用信息安全产品和测评机构的；⑩ 未定期开展自查的；⑪ 违反《管理办法》其他规定的。

6.2.4 检查工作要求

公安机关开展检查工作，应当按照“严格依法、热情服务”的原则，遵守检查纪律，规范检查程序，主动、热情地为运营使用单位提供服务和指导。

要按照“谁受理备案、谁负责检查”的原则，对跨省或者全国联网运行、跨市或者全省联网运行等跨地域的信息系统，由部、省、市级公安机关分别对所受理备案的信息系统进行检查。对辖区内独自运行的信息系统，由受理备案的公安机关独自进行检查。

对于有主管部门的，公安机关要积极会同主管部门开展检查工作，充分发挥主管部门的作用，建立监督检查的配合机制。因故无法会同的，公安机关可以自行开展检查。

对备案单位重要信息系统发生的事件、案件及时进行调查和立案侦查，并指导其开展应急处置工作，为备案单位重要信息系统安全提供有力支持。

APPENDIX

A

附录 A　关于信息安全等级保护工作的实施意见

公　　安　　部
国　家　保　密　局
国 家 密 码 管 理 局　文件
国务院信息化工作办公室

公通字[2004]66 号

关于印发《关于信息安全等级保护工作的实施意见》的通知

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理委员会办公室、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理委员会办公室、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室，各人民团体保密委员会办公室：

《关于信息安全等级保护工作的实施意见》已经国家网络与信息安全协调小组第

三次会议讨论通过，现印发给你们，请认真贯彻实施。

公安部　　国家保密局

国家密码管理委员会办公室　　国务院信息化工作办公室

二〇〇四年九月十五日

主题词：信息 安全 等级 保护 实施 意见

抄送：中央办公厅，国务院办公厅。中央政法委、中央 610 办公室，发展改革委、教育部、科技部、安全部、财政部、信息产业部、铁道部、中国人民银行、海关总署、税务总局、民航总局、广电总局、国务院新闻办、中国证券监督管理委员会，国家电网公司。

公安部办公厅　　2004 年 9 月 17 日印发

承办人：郭启全　　校对：张俊兵

关于信息安全等级保护工作的实施意见

信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息系统安全建设更加突出重点、统一规范、科学合理，对促进我国信息安全的发展将起到重要的推动作用。

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

一、开展信息安全等级保护工作的重要意义

近年来，党中央、国务院高度重视，各有关方面协调配合、共同努力，我国信息安全保障工作取得了很大进展。但是从总体上看，我国的信息安全保障工作尚处于起步阶段，基础薄弱，水平不高，存在以下突出问题：信息安全意识和安全防范能力薄弱，信息安全滞后于信息化发展；信息系统安全建设和管理的目标不明确；信息安全保障工作的重点不突出；信息安全监督管理缺乏依据和标准，监管措施有待到位，监管体系尚待完善。随着信息技术的高速发展和网络应用的迅速普及，我国国民经济和社会信息化进程全面加快，信息系统的基础性、全局性作用日益增强，

信息资源已经成为国家经济建设和社会发展的重要战略资源之一。保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化发展中迫切需要解决的重大问题。

实施信息安全等级保护，能够有效地提高我国信息和信息系统安全建设的整体水平，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于为信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效控制信息安全建设成本；有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。

二、信息安全等级保护制度的原则

信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则。

（一）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

（二）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

（三）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（四）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、

检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括：国家事务处理信息系统（党政机关办公系统）；财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统；教育、国家科研等单位的信息系统；公用通信、广播电视传输等基础信息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其他领域的重要信息系统。

三、信息安全等级保护制度的基本内容

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

信息系统是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级共分五级。

（1）第一级为自主保护级，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。

（2）第二级为指导保护级，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。

（3）第三级为监督保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。

（4）第四级为强制保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。

（5）第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。第一级依照国家管理规范和技术标准进行自主保护；第二级在信息安全监管职能部门指导下依照国家管理规范和技术标准进行自主保护；第三级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查；第四级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查；第五级依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督。

国家对信息安全产品的使用实行分等级管理。

信息安全事件实行分等级响应、处置的制度。依据信息安全事件对信息和信息系统的破坏程度、所造成的社会影响以及涉及的范围，确定事件等级。根据不同安全保护等级的信息系统中发生的不同等级事件制定相应的预案，确定事件响应和处置的范围、程度以及适用的管理制度等。信息安全事件发生后，分等级按照预案响应和处置。

四、信息安全等级保护工作职责分工

公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门

负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。

在信息安全等级保护工作中，涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。

信息和信息系统的主管部门及运营、使用单位按照等级保护的管理规范和技术标准进行信息安全建设和管理。

国务院信息化工作办公室负责信息安全等级保护工作中部门间的协调。

五、实施信息安全等级保护工作的要求

信息安全等级保护工作要突出重点、分级负责、分类指导、分步实施，按照谁主管谁负责、谁运营谁负责的要求，明确主管部门以及信息系统建设、运行、维护、使用单位和个人的安全责任，分别落实等级保护措施。实施信息安全等级保护应当做好以下六个方面工作。

（一）完善标准，分类指导。制定系统完整的信息安全等级保护管理规范和技术标准，并根据工作开展的实际情况不断补充完善。信息安全监管职能部门对不同重要程度的信息和信息系统的安全等级保护工作给予相应的指导，确保等级保护工作顺利开展。

（二）科学定级，严格备案。信息和信息系统的运营、使用单位按照等级保护的管理规范和技术标准，确定其信息和信息系统的安全保护等级，并报其主管部门审批同意。

对于包含多个子系统的信息系统，在保障信息系统安全互联和有效信息共享的前提下，应当根据等级保护的管理规定、技术标准和信息系统内各子系统的重要程度，分别确定安全保护等级。跨地域的大系统实行纵向保护和属地保护相结合的方式。

国务院信息化工作办公室组织国内有关信息安全专家成立信息安全保护等级专

家评审委员会。重要的信息和信息系统的运营、使用单位及其主管部门在确定信息和信息系统的安全保护等级时，应请信息安全保护等级专家评审委员会给予咨询评审。

安全保护等级在三级以上的信息系统，由运营、使用单位报送本地区地市级公安机关备案。跨地域的信息系统由其主管部门向其所在地的同级公安机关进行总备案，分系统分别由当地运营、使用单位向本地地市级公安机关备案。

信息安全产品使用的分等级管理以及信息安全事件分等级响应、处置的管理办法由公安部会同保密局、国密办、信息产业部和认监委等部门制定。

（三）建设整改，落实措施。对已有的信息系统，其运营、使用单位根据已经确定的信息安全保护等级，按照等级保护的管理规范和技术标准，采购和使用相应等级的信息安全产品，建设安全设施，落实安全技术措施，完成系统整改。对新建、改建、扩建的信息系统应当按照等级保护的管理规范和技术标准进行信息系统的规划设计、建设施工。

（四）自查自纠，落实要求。信息和信息系统的运营、使用单位及其主管部门按照等级保护的管理规范和技术标准，对已经完成安全等级保护建设的信息系统进行检查评估，发现问题及时整改，加强和完善自身信息安全等级保护制度的建设，加强自我保护。

（五）建立制度，加强管理。信息和信息系统的运营、使用单位按照与本系统安全保护等级相对应的管理规范和技术标准的要求，定期进行安全状况检测评估，及时消除安全隐患和漏洞，建立安全制度，制定不同等级信息安全事件的响应、处置预案，加强信息系统的安全管理。信息和信息系统的主管部门应当按照等级保护的管理规范和技术标准的要求做好监督管理工作，发现问题，及时督促整改。

（六）监督检查，完善保护。公安机关按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息和信息系统的安全等级保护状况进行监督检查。发现确定的安全保护等级不符合等级保护的管理规范和技术标准的，要通知信息和信息系统的主管部门及运营、使用单位进行整改；发现存在安全隐患或未达到等级保护

的管理规范和技术标准要求的，要限期整改，使信息和信息系统的安全保护措施更加完善。对信息系统中使用的信息安全产品的等级进行监督检查。

对第五级信息和信息系统的监督检查，由国家指定的专门部门、专门机构按照有关规定进行。

国家保密工作部门、密码管理部门以及其他职能部门按照职责分工指导、监督、检查。

六、信息安全等级保护工作实施计划

计划用三年左右的时间在全国范围内分三个阶段实施信息安全等级保护制度。

（一）准备阶段。为了保障信息安全等级保护制度的顺利实施，在全面实施等级保护制度之前，用一年左右的时间做好下列准备工作。

（1）加强领导，落实责任。在国家网络与信息安全协调小组的领导下，地方各级人民政府、信息安全监管职能部门、信息系统的主管部门和运营、使用单位要明确各自的安全责任，建立协调配合机制，分别制定详细的实施方案，积极推进信息安全等级保护制度的建立，推动信息安全管理运行机制的建立和完善。

（2）加快完善法律法规和标准体系。法律规范和技术标准是推广和实施信息安全等级保护工作的法律依据和技术保障。为此，《信息安全等级保护管理办法》和《信息安全等级保护实施指南》、《信息安全等级保护评估指南》等法规、规范要加紧制定，尽快出台。

加快信息安全等级保护管理与技术标准的制定和完善，其他现行的相关标准规范中与等级保护管理规范和技术标准不相适应的，应当进行调整。

（3）建设信息安全等级保护监督管理队伍和技术支撑体系。信息安全监管职能部门要建立专门的信息安全等级保护监督检查机构，充实力量，加强建设，抓紧培训，使监督检查人员能够全面掌握信息安全等级保护相关法律规范和管理规范及技

术标准，熟练运用技术工具，切实承担信息安全等级保护的指导、监督、检查职责。同时，还要建立信息安全等级保护监督、检查工作的技术支撑体系，组织研制、开发科学、实用的检查、评估工具。

（4）进一步做好等级保护试点工作。选择电子政务、电子商务以及其他方面的重点单位开展等级保护试点工作，并在试点工作的基础上进一步完善等级保护实施指南等相关的配套规范、标准和工具，积累信息安全等级保护工作实施的方法和经验。

（5）加强宣传、培训工作。地方各级人民政府、信息安全监管职能部门和信息系统的主管部门要积极宣传信息安全等级保护的相关法规、标准和政策，组织开展相关培训，提高对信息安全等级保护工作的认识和重视，积极推动各有关部门、单位做好开展信息安全等级保护工作的前期准备。

（二）重点实行阶段。在做好前期准备工作的基础上，用一年左右的时间，在国家重点保护的涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统中实行等级保护制度。经过一年的建设，使基础信息网络和重要信息系统的核心要害部位得到有效保护，涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统的保护状况得到较大改善，结束目前基本没有保护措施或保护措施不到位的状况。

在工作中，如发现等级保护的管理规范和技术标准以及检查评估工具等存在问题，及时组织有关部门进行调整和修订。

（三）全面实行阶段。在试行工作的基础上，用一年左右的时间，在全国全面推行信息安全等级保护制度。已经实施等级保护制度的信息和信息系统的运营、使用单位及其主管部门，要进一步完善信息安全保护措施。没有实施等级保护制度的，要按照等级保护的管理规范和技术标准认真组织落实。

经过三年的努力，逐步将信息安全等级保护制度落实到信息安全规划、建设、评估、运行维护等各个环节，使我国信息安全保障状况得到基本改善。

APPENDIX

B

附录 B　信息安全等级保护管理办法

公　　安　　部
国　家　保　密　局
国 家 密 码 管 理 局　文件
国务院信息化工作办公室

公通字[2007]43 号

关于印发《信息安全等级保护管理办法》的通知

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理局（国家密码管理委员会办公室）、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室，各人民团体保密委员会办公室：

为加快推进信息安全等级保护，规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定了《信息安全

等级保护管理办法》。现印发给你们，请认真贯彻执行。

公安部　　国家保密局

国家密码管理局　　国务院信息化工作办公室

二〇〇七年六月二十二日

主题词：信息 安全 等级 保护 管理 办法

抄送：中央办公厅、国务院办公厅。

中央和国家机关各部委、国务院各直属机构、办事机构、事业单位，国务院部委管理的各国家局。

国家保密局、国家密码管理局、国务院信息化工作办公室有关部门。

公安部党委、部属有关局级单位。

（存档3份　共印2500份）

公安部办公厅　　2007年6月26日印发

承办人：郭启全　　刘　伟　　校对：郭启全

信息安全等级保护管理办法

第一章　总则

第一条　为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。

第二条　国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条　公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

第四条　信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条　信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章　等级划分与保护

第六条　国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织

的合法权益的危害程度等因素确定。

第七条 信息系统的安全保护等级分为以下五级。

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊

安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章　等级保护的实施与管理

第九条　信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条　信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条　信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十二条　在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859—1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术 信息系统通用安全技术要求》（GB/T20271—2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270—2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272—2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273—2006）、《信息安全技术 服务器技术要求》、《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671—2006）等技术标准同步建设符合该等级要求的信息安全设施。

第十三条　运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》（GB/T20269—2006）、《信息安全技术 信息系统安全工程管理要求》（GB/T20282—

2006）、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十五条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

（一）系统拓扑结构及说明；

（二）系统安全组织机构和管理制度；

（三）系统安全保护设施设计实施方案或者改建实施方案；

（四）系统使用的信息安全产品清单及其认证、销售许可证明；

（五）测评后符合系统安全保护等级的技术检测评估报告；

（六）信息系统安全保护等级专家评审意见；

（七）主管部门审核批准信息系统安全保护等级的意见。

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的，应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。

对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查：

（一）信息系统安全需求是否发生变化，原定保护等级是否准确；

（二）运营、使用单位安全管理制度、措施的落实情况；

（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；

（四）系统安全等级测评是否符合要求；

（五）信息安全产品使用是否符合要求；

（六）信息系统安全整改情况；

（七）备案材料与运营、使用单位、信息系统的符合情况；

（八）其他应当进行监督检查的事项。

第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件：

（一）信息系统备案事项变更情况；

（二）安全组织、人员的变动情况；

（三）信息安全管理制度、措施变更情况；

（四）信息系统运行状况记录；

（五）运营、使用单位及主管部门定期对信息系统安全状况的检查记录；

（六）对信息系统开展等级测评的技术测评报告；

（七）信息安全产品使用的变更情况；

（八）信息安全事件应急预案，信息安全事件应急处置结果报告；

（九）信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

（五）对国家安全、社会秩序、公共利益不构成危害；

（六）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）从事相关检测评估工作两年以上，无违法记录；

（四）工作人员仅限于中国公民；

（五）法人及主要业务、技术人员无犯罪记录；

（六）使用的技术装备、设施应当符合本办法对信息安全产品的要求；

（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

（八）对国家安全、社会秩序、公共利益不构成威胁。

第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务：

（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；

（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；

（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第四章　涉及国家秘密信息系统的分级保护管理

第二十四章　涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。

第二十五条　涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17—2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条　涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条　涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分

级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行检测，通过检测的产品由国家保密局审核发布目录。

第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准 BMB22—2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。

涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：

（一）系统设计、实施方案及审查论证意见；

（二）系统承建单位资质证明材料；

（三）系统建设和工程监理情况报告；

（四）系统安全保密检测评估报告；

（五）系统安全保密组织机构和管理制度情况；

（六）其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准BMB20—2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作：

（一）指导、监督和检查分级保护工作的开展；

（二）指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级；

（三）参与涉密信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计；

（四）依法对涉密信息系统集成资质单位进行监督管理；

（五）严格进行系统测评和审批工作，监督检查涉密信息系统建设使用单位分级保护管理制度和技术措施的落实情况；

（六）加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评；

（七）了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

第五章 信息安全等级保护的密码管理

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级

保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责

令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果。

（一）未按本办法规定备案、审批的；

（二）未按本办法规定落实安全管理制度、措施的；

（三）未按本办法规定开展系统安全状况检查的；

（四）未按本办法规定开展系统安全技术测评的；

（五）接到整改通知后，拒不整改的；

（六）未按本办法规定选择使用信息安全产品和测评机构的；

（七）未按本办法规定如实提供有关文件和证明材料的；

（八）违反保密管理规定的；

（九）违反密码管理规定的；

（十）违反本办法其他规定的。

违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。

第四十一条 信息安全监管部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第七章 附则

第四十二条 已运行信息系统的运营、使用单位自本办法施行之日起 180 日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

第四十三条 本办法所称“以上”包含本数（级）。

第四十四条 本办法自发布之日起施行，《信息安全等级保护管理办法（试行）》（公通字[2006]7 号）同时废止。

APPENDIX

C

附录 C　关于开展全国重要信息系统安全等级保护定级工作的通知

中华人民共和国公安部

国　家　保　密　局

国 家 密 码 管 理 局

国务院信息化工作办公室

关于开展全国重要信息系统安全等级保护定级工作的通知

公信安[2007]861 号

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理局（国家密码管理委员会办公室）、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室，各人民团体保密委员会办公室：

为进一步贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》和公安部、国家保密局、国家密码管理局、国务院信息化工作办公室《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》（以下简称《管理办法》）精神，提高我国基础信息网络和重要信息系统的信息安全保护能力和水平，根据国家网络与信息安全协调小组 2007 年的工作部署，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室定于 2007 年 7 月至 10 月在全国范围内组织开展重要信息系统安全等级保护定级工作（以下简称“定级工作”）。现就有关事项通知如下。

一、定级范围

（一）电信、广电行业的公用通信网、广播电视传输网等基础信息网络，经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统。

（二）铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源、能源、交通、文化、教育、统计、工商行政管理、邮政等行业、部门的生产、调度、管理、办公等重要信息系统。

（三）市（地）级以上党政机关的重要网站和办公信息系统。

（四）涉及国家秘密的信息系统（以下简称涉密信息系统）。

二、定级工作的主要内容

（一）开展信息系统基本情况的摸底调查。各行业主管部门、运营使用单位要组织开展对所属信息系统的摸底调查，全面掌握信息系统的数量、分布、业务类型、应用或服务范围、系统结构等基本情况，按照《管理办法》和《信息系统安全等级保护定级指南》的要求，确定定级对象。各行业主管部门要根据行业特点提出指导本地区、本行业定级工作的具体意见。

（二）初步确定安全保护等级。各信息系统主管部门和运营使用单位要按照《管理办法》和《信息系统安全等级保护定级指南》，初步确定定级对象的安全保护等级，起草定级报告（报告模版见附件 1）。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。涉密信息系统的等级确定按照国家保密局的有关规定和标准执行。

（三）评审与审批。初步确定信息系统安全保护等级后，可以聘请专家进行评审。对拟确定为第四级以上信息系统的，由运营使用单位或主管部门请国家信息安全保护等级专家评审委员会评审。运营使用单位或主管部门参照评审意见最后确定信息系统安全保护等级，形成定级报告。当专家评审意见与信息系统运营使用单位或其主管部门意见不一致时，由运营使用单位或主管部门自主决定信息系统安全保护等级。信息系统运营使用单位有上级行业主管部门的，所确定的信息系统安全保护等级应当报经上级行业主管部门审批同意。

（四）备案。根据《管理办法》，信息系统安全保护等级为第二级以上的信息系统运营使用单位或主管部门到公安部网站下载《信息系统安全等级保护备案表》（见附件 2）和辅助备案工具，持填写的备案表和利用辅助备案工具生成的备案电子数据，到公安机关办理备案手续，提交有关备案材料及电子数据文件。其中，第二级信息系统的备案单位只需要填写备案表中的表一和表二，第三级以上信息系统的备案单位还应当提交备案表附件所列各项内容的书面材料。隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。

涉密信息系统建设使用单位依据《管理办法》和国家保密局的有关规定，填写《涉及国家秘密的信息系统分级保护备案表》（见附件 3），按照属地化管理原则，中央和国家机关单位的涉密信息系统向国家保密局备案；地方单位的涉密信息系统向所在地的市（地）级以上保密工作部门备案；中央和国家机关地方所属单位的涉密信息系统，向所在地的省级保密工作部门备案。

（五）备案管理。公安机关和国家保密工作部门负责受理备案并进行备案管理。信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，颁发信息系统安全保护等级备案证明。发现不符合《管理办法》及有关标准的，应当通知备案单位予以纠正。发现定级不准的，应当通知运营使用单位或其主管部门重新审核确定。各级保密工作部门加强对涉密信息系统定级工作的指导、监督和检查。

三、定级工作的要求

（一）加强领导，落实保障。各地区、各部门要加强对本地区、本行业信息安全等级保护工作的组织领导，及时掌握工作进展情况，并可组织成立专家组，明确技术支持力量。信息系统运营使用单位要成立等级保护工作组，落实责任部门、责任人员和经费，保障定级工作顺利进行。

（二）明确责任，密切配合。定级工作由各级公安机关牵头，会同国家保密工作部门、国家密码管理部门和信息化领导小组办事机构共同组织实施。公安机关负责定级工作的监督、检查、指导；国家保密工作部门负责涉密系统定级工作的监督、检查、指导；国家密码管理部门负责定级工作中有关密码工作的监督、检查、指导；信息化领导小组办事机构负责定级工作的部门间协调。各信息系统主管部门组织本行业、本部门信息系统运营使用单位开展定级工作，督促其落实定级工作各项任务。各信息系统运营使用单位依据《管理办法》和本通知要求，具体实施定级工作。

（三）动员部署，开展培训。各地区、各部门要按照统一部署广泛进行宣传动员，举办形式多样的培训班、研讨班等，层层培训。公安部会同国家保密局、国家密码管理局、国务院信息化工作办公室对国家有关部委、各省级公安、保密、密码和信息化领导小组办事机构就《管理办法》和《信息系统安全等级保护定级指南》等内容进行培训。信息系统主管部门对所管辖的信息系统运营使用单位进行培训。各地参照上述培训模式开展培训工作。

（四）及时总结，提出建议。各地区、各部门要结合本地区、本行业开展定级工作的实际，认真总结经验和不足，提出改进和完善定级方法的意见和建议。各地区、各部门负责等级保护的领导机构要及时总结定级工作经验，形成定级工作总结报告，并及时报送公安部。涉密系统定级工作总结报告向国家保密局报送。

此次定级工作完成后，请各主管部门、运营使用单位按照《管理办法》和有关技术标准，继续开展信息系统安全等级保护的系统建设或整改、等级测评、自查自纠等后续工作，各级公安、保密、密码部门要开展等级保护工作的监督、检查和指导。

执行中有何问题，请及时报告。

公安部联系人郭启全，联系电话：010-66261745。

国家保密局联系人魏力，联系电话：010-83086085。

国家密码管理局联系人王家玮，联系电话：010-83084734。

国务院信息办联系人李强，联系电话：010-83083664。

公安部网址：www.mps.gov.cn(互联网)；

ftp://10.1.185.68（公安网）。

技术咨询电话：010-88530013、88530015。

附件 1：《信息系统安全等级保护定级报告》模版

附件 2：《信息系统安全等级保护备案表》

附件 3：《涉及国家秘密的信息系统分级保护备案表》

附件1：

信息系统安全等级保护定级报告

一、×××信息系统描述

简述确定该系统为定级对象的理由。从三个方面进行说明：一是描述承担信息系统安全责任的相关单位或部门，说明本单位或部门对信息系统具有信息安全保护责任，该信息系统为本单位或部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务以及业务情况描述。

二、×××信息系统安全保护等级确定（定级方法参见国家标准《信息系统安全等级保护定级指南》）

（一）业务信息安全保护等级的确定

1．业务信息描述

描述信息系统处理的主要业务信息等。

2．业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3．信息受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4．业务信息安全等级的确定

依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级。

（二）系统服务安全保护等级的确定

1．系统服务描述

描述信息系统的服务范围、服务对象等。

2．系统服务受到破坏时所侵害客体的确定

说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3．系统服务受到破坏后对侵害客体的侵害程度的确定

说明系统服务受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4．系统服务安全等级的确定

依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级。

（三）安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定×××系统安全保护等级为第几级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
×××信息系统	×	×	×

附件 2：

备案表编号：□□□□□□—□□□□□

信息系统安全等级保护备案表

备 案 单 位：_____（盖章）_____

备 案 日 期：_____

受理备案单位：_____（盖章）_____

受 理 日 期：_____

中华人民共和国公安部监制

填 表 说 明

一、制表依据。根据《信息安全等级保护管理办法》（公通字[2007]43 号）的规定，制作本表。

二、填表范围。本表由第二级以上信息系统运营使用单位或主管部门（以下简称“备案单位”）填写；本表由四张表单构成，表一为单位信息，每个填表单位填写一张；表二为信息系统基本信息，表三为信息系统定级信息，表二、表三每个信息系统填写一张；表四为第三级以上信息系统需要同时提交的内容，由每个第三级以上信息系统填写一张，并在完成系统建设、整改、测评等工作，投入运行后 30 日内向受理备案公安机关提交；表二、表三、表四可以复印使用。

三、保存方式。本表一式两份，一份由备案单位保存，一份由受理备案公安机关存档。

四、本表中有选择的地方请在选项左侧“□”内画“√”，如选择“其他”，请在其后的横线中注明详细内容。

五、封面中备案表编号（由受理备案的公安机关填写并校验）：分两部分共 11 位，第一部分 6 位，为受理备案公安机关代码前 6 位（可参照行标 GA380—2002）。第二部分 5 位，为受理备案的公安机关给出的备案单位的顺序编号。

六、封面中备案单位：是指负责运营使用信息系统的法人单位全称。

七、封面中受理备案单位：是指受理备案的公安机关公共信息网络安全监察部门名称。此项由受理备案的公安机关负责填写并盖章。

八、表一“04 行政区划代码”：是指备案单位所在的地（区、市、州、盟）行政区划代码。

九、表一“05 单位负责人”：是指主管本单位信息安全工作的领导。

十、表一“06 责任部门”：是指单位内负责信息系统安全工作的部门。

十一、表一“08 隶属关系”：是指信息系统运营使用单位与上级行政机构的从属关系，须按照单位隶属关系代码（GB/T12404—1997）填写。

十二、表二“02 系统编号”：是由运营使用单位给出的本单位备案信息系统的编号。

十三、表二“05 系统网络平台”：是指系统所处的网络环境和网络构架情况。

十四、表二“07 关键产品使用情况”：国产品是指系统中该类产品的研制、生产单位是由中国公民、法人投资或者国家投资或者控股，在中华人民共和国境内具有独立的法人资格，产品的核心技术、关键部件具有我国自主知识产权。

十五、表二“08 系统采用服务情况”：国内服务商是指服务机构在中华人民共和国境内注册成立（港澳台地区除外），由中国公民、法人或国家投资的企事业单位。

十六、表三 01、02、03 项：填写上述三项内容，确定信息系统安全保护等级时可参考《信息系统安全等级保护定级指南》，信息系统安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。01、02 项中每一个确定的级别所对应的损害客体及损害程度可多选。

十六、表三“06 主管部门”：是指对备案单位信息系统负领导责任的行政或业务主管单位或部门。部级单位此项可不填。

十七、解释：本表由公安部公共信息网络安全监察局监制并负责解释，未经允许，任何单位和个人不得对本表进行改动。

表一　单位基本情况

<table>
<tr><td>01 位名称</td><td colspan="8"></td></tr>
<tr><td>02 单位地址</td><td colspan="8">省(自治区、直辖市)　　地(区、市、州、盟)
县(区、市、旗)</td></tr>
<tr><td>03 邮政编码</td><td colspan="3"></td><td colspan="2">04 行政区划代码</td><td colspan="3"></td></tr>
<tr><td rowspan="2">05 单位负责人</td><td>姓　名</td><td colspan="2"></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td><td>电子邮件</td><td colspan="3"></td></tr>
<tr><td>06 责任部门</td><td colspan="8"></td></tr>
<tr><td rowspan="3">07 责任部门联系人</td><td>姓　名</td><td colspan="2"></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td><td rowspan="2">电子邮件</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>移动电话</td><td colspan="2"></td></tr>
<tr><td>08 隶属关系</td><td colspan="8">□1 中央　□2 省(自治区、直辖市)　□3 地(区、市、州、盟)
□4 县（区、市、旗）　□9 其他</td></tr>
<tr><td>09 单位类型</td><td colspan="8">□1 党委机关　□2 政府机关　□3 事业单位　□4 企业　□9 其他</td></tr>
<tr><td>10 行业类别</td><td colspan="8">□11 电信　□12 广电　□13 经营性公众互联网
□21 铁路　□22 银行　□23 海关　□24 税务
□25 民航　□26 电力　□27 证券　□28 保险
□31 国防科技工业　□32 公安　□33 人事劳动和社会保障　□34 财政
□35 审计　□36 商业贸易　□37 国土资源　□38 能源
□39 交通　□40 统计　□41 工商行政管理　□42 邮政
□43 教育　□44 文化　□45 卫生　□46 农业
□47 水利　□48 外交　□49 发展改革　□50 科技
□51 宣传　□52 质量监督检验检疫
□99 其他</td></tr>
<tr><td rowspan="2">11 信息系统总数</td><td rowspan="2">个</td><td>12 第二级信息系统数</td><td>个</td><td>13 第三级信息系统数</td><td>个</td><td colspan="2"></td></tr>
<tr><td>14 第四级信息系统数</td><td>个</td><td>15 第五级信息系统数</td><td>个</td><td colspan="2"></td></tr>
</table>

表二（ / ）信息系统情况

<table>
<tr><td colspan="2">01 系统名称</td><td colspan="5"></td><td>02 系统编号</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">03 系统承载业务情况</td><td>业务类型</td><td colspan="9">□1 生产作业 □2 指挥调度 □3 管理控制 □4 内部办公
□5 公众服务 □9 其他</td></tr>
<tr><td>业务描述</td><td colspan="9"></td></tr>
<tr><td rowspan="3">04 系统服务情况</td><td rowspan="2">服务范围</td><td colspan="9">□10 全国 □11 跨省（区、市） 跨 个
□20 全省（区、市） □21 跨地（市、区） 跨 个
□30 地（市、区）内
□99 其他</td></tr>
<tr><td>服务对象</td><td colspan="9">□1 单位内部人员 □2 社会公众人员 □3 两者均包括 □9 其他</td></tr>
<tr><td rowspan="2">05 系统网络平台</td><td>覆盖范围</td><td colspan="9">□1 局域网 □2 城域网 □3 广域网 □9 其他</td></tr>
<tr><td>网络性质</td><td colspan="9">□1 业务专网 □2 互联网 □9 其他</td></tr>
<tr><td colspan="2">06 系统互联情况</td><td colspan="9">□1 与其他行业系统连接 □2 与本行业其他单位系统连接
□3 与本单位其他系统连接 □9 其他</td></tr>
<tr><td colspan="2" rowspan="8">07 关键产品使用情况</td><td rowspan="2">序号</td><td rowspan="2">产品类型</td><td rowspan="2">数量</td><td colspan="6">使用国产品率</td></tr>
<tr><td colspan="2">全部使用</td><td colspan="2">全部未使用</td><td colspan="2">部分使用及使用率</td></tr>
<tr><td>1</td><td>安全专用产品</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td>2</td><td>网络产品</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td>3</td><td>操作系统</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td>4</td><td>数据库</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td>5</td><td>服务器</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td>6</td><td>其他</td><td></td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□ %</td></tr>
<tr><td colspan="2" rowspan="9">08 系统采用服务情况</td><td rowspan="2">序号</td><td colspan="2" rowspan="2">服务类型</td><td colspan="6">服务责任方类型</td></tr>
<tr><td colspan="2">本行业（单位）</td><td colspan="2">国内其他服务商</td><td colspan="2">国外服务商</td></tr>
<tr><td>1</td><td colspan="2">等级测评 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>2</td><td colspan="2">风险评估 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>3</td><td colspan="2">灾难恢复 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>4</td><td colspan="2">应急响应 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>5</td><td colspan="2">系统集成 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>6</td><td colspan="2">安全咨询 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>7</td><td colspan="2">安全培训 □有□无</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td>8</td><td colspan="2">其他</td><td colspan="2">□</td><td colspan="2">□</td><td colspan="2">□</td></tr>
<tr><td colspan="2">09 等级测评单位名称</td><td colspan="9"></td></tr>
<tr><td colspan="2">10 何时投入运行使用</td><td colspan="9">年 月 日</td></tr>
<tr><td colspan="2">11 系统是否是分系统</td><td colspan="9">□是 □否（如选择是请填下两项）</td></tr>
<tr><td colspan="2">12 上级系统名称</td><td colspan="9"></td></tr>
<tr><td colspan="2">13 上级系统所属单位名称</td><td colspan="9"></td></tr>
</table>

表三（ / ）信息系统定级情况

<table>
<tr><td rowspan="6">01 确定业务信息安全保护等级</td><td>损害客体及损害程度</td><td>级别</td></tr>
<tr><td>□仅对公民、法人和其他组织的合法权益造成损害</td><td>□第一级</td></tr>
<tr><td>□对公民、法人和其他组织的合法权益造成严重损害
□对社会秩序和公共利益造成损害</td><td>□第二级</td></tr>
<tr><td>□对社会秩序和公共利益造成严重损害
□对国家安全造成损害</td><td>□第三级</td></tr>
<tr><td>□对社会秩序和公共利益造成特别严重损害
□对国家安全造成严重损害</td><td>□第四级</td></tr>
<tr><td>□对国家安全造成特别严重损害</td><td>□第五级</td></tr>
<tr><td rowspan="5">02 确定系统服务安全保护等级</td><td>□仅对公民、法人和其他组织的合法权益造成损害</td><td>□第一级</td></tr>
<tr><td>□对公民、法人和其他组织的合法权益造成严重损害
□对社会秩序和公共利益造成损害</td><td>□第二级</td></tr>
<tr><td>□对社会秩序和公共利益造成严重损害
□对国家安全造成损害</td><td>□第三级</td></tr>
<tr><td>□对社会秩序和公共利益造成特别严重损害
□对国家安全造成严重损害</td><td>□第四级</td></tr>
<tr><td>□对国家安全造成特别严重损害</td><td>□第五级</td></tr>
<tr><td colspan="2">03 信息系统安全保护等级</td><td>□第一级 □第二级 □第三级 □第四级 □第五级</td></tr>
<tr><td colspan="2">04 定级时间</td><td>年 月 日</td></tr>
<tr><td colspan="2">05 专家评审情况</td><td>□已评审 □未评审</td></tr>
<tr><td colspan="2">06 是否有主管部门</td><td>□有 □无（如选择有请填下两项）</td></tr>
<tr><td colspan="2">07 主管部门名称</td><td></td></tr>
<tr><td colspan="2">08 主管部门审批定级情况</td><td>□已审批 □未审批</td></tr>
<tr><td colspan="2">09 系统定级报告</td><td>□有 □无 附件名称_____</td></tr>
<tr><td colspan="2">填表人：</td><td>填表日期： 年 月 日</td></tr>
</table>

备案审核民警： 审核日期： 年 月 日

表四（ / ）第三级以上信息系统提交材料情况

01 系统拓扑结构及说明	□有	□无	附件名称_____
02 系统安全组织机构及管理制度	□有	□无	附件名称_____
03 系统安全保护设施设计实施方案或改建实施方案	□有	□无	附件名称_____
04 系统使用的安全产品清单及认证、销售许可证明	□有	□无	附件名称_____
05 系统等级测评报告	□有	□无	附件名称_____
06 专家评审情况	□有	□无	附件名称_____
07 上级主管部门审批意见	□有	□无	附件名称_____

附件 3:

涉及国家秘密的信息系统分级保护备案表

单位名称	
涉密信息系统名称	
系统密级（保护等级）	□ 秘密　　□ 机密　　□ 绝密
系统联接范围	□局域网 □城域网 □广域网（跨____个省或地）
系统安全域划分和安全域密级确定	□未划分安全域 □划分安全域（共有____个，其中绝密级____个， 机密级____个，秘密级____个，内部级____个）
系统主要承建单位	
系统投入使用时间	
系统运行管理部门	
系统安全保密管理部门	
系统分级保护实施情况	□已经实施　□正在实施　□计划_____年实施

填报日期：　　年　月　日　　填报单位：（盖章）

填表说明：

1．“系统密级”依据《涉及国家秘密的信息系统分级保护管理办法》和国家保密标准 BMB17—2006 确定。

2．涉密信息系统一般应划分安全域，同一系统内的不同安全域根据所处理信息的重要程度，可分别确定密级。

3．表中“□”项，确认画“√”。

4．填报多个涉密信息系统，可复印此表。

国家保密局制

APPENDIX

D

附录 D　信息安全等级保护备案实施细则（试行）

中 华 人 民 共 和 国 公 安 部

关于印发《信息安全等级保护备案实施细则》的通知

公信安[2007]1360 号

各省、自治区、直辖市公安厅（局）公共信息网络安全监察总队（处），新疆生产建设兵团公安局公共信息网络安全监察处：

为配合《信息安全等级保护管理办法》（公通字[2007]43 号）和《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）的贯彻实施，严格规范备案管理工作，实现备案工作的规范化、制度化，我局制定了《信息安全等级保护备案实施细则》及配套法律文书，现印发给你们，请认真贯彻执行。

二〇〇七年十月二十六日

信息安全等级保护备案实施细则

第一条 为加强和指导信息安全等级保护备案工作，规范备案受理、审核和管理等工作，根据《信息安全等级保护管理办法》制定本实施细则。

第二条 本细则适用于非涉及国家秘密的第二级以上信息系统的备案。

第三条 地市级以上公安机关公共信息网络安全监察部门受理本辖区内备案单位的备案。隶属于省级的备案单位，其跨地（市）联网运行的信息系统，由省级公安机关公共信息网络安全监察部门受理备案。

第四条 隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由公安部公共信息网络安全监察局受理备案，其他信息系统由北京市公安局公共信息网络安全监察部门受理备案。

隶属于中央的非在京单位的信息系统，由当地省级公安机关公共信息网络安全监察部门（或其指定的地市级公安机关公共信息网络安全监察部门）受理备案。

跨省或者全国统一联网运行并由主管部门统一定级的信息系统在各地运行、应用的分支系统（包括由上级主管部门定级，在当地有应用的信息系统），由所在地地市级以上公安机关公共信息网络安全监察部门受理备案。

第五条 受理备案的公安机关公共信息网络安全监察部门应该设立专门的备案窗口，配备必要的设备和警力，专门负责受理备案工作，受理备案地点、时间、联系人和联系方式等应向社会公布。

第六条 信息系统运营、使用单位或者其主管部门（以下简称“备案单位”）应当在信息系统安全保护等级确定后 30 日内，到公安机关公共信息网络安全监察部门办理备案手续。办理备案手续时，应当首先到公安机关指定的网址下载并填写备案表，准备好备案文件，然后到指定的地点备案。

第七条 备案时应当提交《信息系统安全等级保护备案表》（以下简称《备案表》）（一式两份）及其电子文档。第二级以上信息系统备案时需提交《备案表》中的表一、表二、表三；第三级以上信息系统还应当在系统整改、测评完成后30日内提交《备案表》表四及其有关材料。

第八条 公安机关公共信息网络安全监察部门收到备案单位提交的备案材料后，对属于本级公安机关受理范围且备案材料齐全的，应当向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案材料不齐全的，应当当场或者在五日内一次性告知其补正内容；对不属于本级公安机关受理范围的，应当书面告知备案单位到有管辖权的公安机关办理。

第九条 接收备案材料后，公安机关公共信息网络安全监察部门应当对下列内容进行审核：

（一）备案材料填写是否完整，是否符合要求，其纸质材料和电子文档是否一致；

（二）信息系统所定安全保护等级是否准确。

第十条 经审核，对符合等级保护要求的，公安机关公共信息网络安全监察部门应当自收到备案材料之日起的十个工作日内，将加盖本级公安机关印章（或等级保护专用章）的《备案表》一份反馈备案单位，一份存档；对不符合等级保护要求的，公安机关公共信息网络安全监察部门应当在十个工作日内通知备案单位进行整改，并出具《信息系统安全等级保护备案审核结果通知》。

第十一条 《备案表》中表一、表二、表三内容经审核合格的，公安机关公共信息网络安全监察部门应当出具《信息系统安全等级保护备案证明》（以下简称《备案证明》）。《备案证明》由公安部统一监制。

第十二条 公安机关公共信息网络安全监察部门对定级不准的备案单位，在通知整改的同时，应当建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。

备案单位仍然坚持原定等级的，公安机关公共信息网络安全监察部门可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关公共信息网络安全监察部门同意后，同时通报备案单位上级主管部门。

第十三条 对拒不备案的，公安机关应当依据《中华人民共和国计算机信息系统安全保护条例》等其他有关法律、法规规定，责令限期整改。逾期仍不备案的，予以警告，并向其上级主管部门通报。

依照前款规定向中央和国家机关通报的，应当报经公安部公共信息网络安全监察局同意。

第十四条 受理备案的公安机关公共信息网络安全监察部门应当及时将备案文件录入到数据库管理系统，并定期逐级上传《备案表》中表一、表二、表三内容的电子数据。上传时间为每季度的第一天。

受理备案的公安机关公共信息网络安全监察部门应当建立管理制度，对备案材料按照等级进行严格管理，严格遵守保密制度，未经批准不得对外提供查询。

第十五条 公安机关公共信息网络安全监察部门受理备案时不得收取任何费用。

第十六条 本细则所称“以上”包含本数（级）。

第十七条 各省（区、市）公安机关公共信息网络安全监察部门可以依据本细则制定具体的备案工作规范，并报公安部公共信息网络安全监察局备案。

接收材料回执编号 J-□□□□□

信息系统安全等级保护
备案材料接收回执

（存根）

备案类型：□初次备案 □变更备案 □其他_____

备案单位：

备案单位联系人： 联系电话：

材料数量：□表一 共 页 □表二 共 页 □表三 共 页
□表四 共 页 □附件 共 份 □电子数据

材料接受人：

接受日期： 年 月 日

接收材料回执编号 J-□□□□□

信息系统安全等级保护
备案材料接收回执

_____：

我单位接收你单位提交的《信息系统安全等级保护备案表》如下具体备案材料（备案日期 年 月 日）：

□表一 共 页 □表二 共 页 □表三 共 页
□表四 共 页 □附件 共 份 □电子数据

我单位将自即日起的___日内，反馈备案审核结果。

接收人：

接收单位（盖章）

年 月 日

业务联系电话：

网址：

备案整改通知编号：S-□□□□□

信息系统安全等级保护
备案审核结果通知

（存根）

备案类型：□初次备案　□变更备案　□其他_____

备案单位：

备案单位联系人：　　联系电话：

审核人：

审核日期：　　年　月　日

备案整改通知编号：S-□□□□□

信息系统安全等级保护
备案审核结果通知

_____：

经对你单位提交的《信息系统安全等级保护备案表》（备案表编号____/____）进行审核，备案材料不符合要求，请你单位按照审核单中所列内容进行整改后，于____天内重新进行备案。

附：《信息系统安全等级保护备案审核详单》

审核人：　　业务联系电话：

审核单位（盖章）

年　月　日

信息系统安全等级保护备案
审核详单

<table>
<tr><td rowspan="2">审核结果一</td><td>01 是否按要求填写《信息系统安全等级保护备案表》</td><td>是□　　否□</td></tr>
<tr><td>02 是否提交《信息系统安全等级保护备案表》电子版</td><td>是□　　否□</td></tr>
<tr><td rowspan="4">审查结果二</td><td>03《信息系统安全等级保护备案表》内容是否完整</td><td>是□　　否□（如否请填写下项）</td></tr>
<tr><td colspan="2">1．表　　第　　项内容不完整；
2．表　　第　　项内容不完整；
3．表　　第　　项内容不完整；
4．表　　第　　项内容不完整；
5．表　　第　　项内容不完整；</td></tr>
<tr><td>04《信息系统安全等级保护备案表》附件内容是否完整</td><td>是□　　否□（如否请填写下项）</td></tr>
<tr><td colspan="2">1．附件　　第　部分内容不完整；
2．附件　　第　部分内容不完整；
3．附件　　第　部分内容不完整；
4．附件　　第　部分内容不完整；
5．附件　　第　部分内容不完整；</td></tr>
<tr><td>审核结果三</td><td colspan="2">1．信息系统_____安全保护等级定级不准确，建议重新审核确定系统安全保护等级；
2．信息系统_____安全保护等级定级不准确，建议重新审核确定系统安全保护等级；
3．信息系统_____安全保护等级定级不准确，建议重新审核确定系统安全保护等级；
（可自行添加）</td></tr>
</table>

（备案证明背版）

注意事项：

1．备案单位备案后应当依据信息系统所定安全保护等级，按照《信息安全等级保护管理办法》中规定的技术标准和管理规范建设安全设施，落实安全保护措施。

2．备案事项发生变更时，备案单位应当自变更之日起三十日内将变更情况报公安机关公共信息网络安全监察部门重新备案。

3．本备案证由信息系统运营使用单位或其主管部门保管，公安机关监督检查时应主动出示本证。

（此处印制公安机关名称）

信息系统安全等级保护限期整改通知书

×公信安 限字[　　] 第　　号

检查时间＿＿＿＿＿＿＿＿＿＿检查地点＿＿＿＿＿＿＿＿＿＿

被检查单位名称＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

被检查单位地址＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

违规行为＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

限期改正时间＿＿＿年＿＿月＿＿＿日至＿＿＿年＿＿＿月＿＿＿日

办理单位＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

承 办 人＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

批 准 人＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

填 发 人＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

填发日期＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

存根

（此处印制公安机关名称）

信息系统安全等级保护限期整改通知书

×公信安 限字[ ]第 号

_____：

根据《中华人民共和国计算机信息系统安全保护条例》，我单位工作人员于_____年___月___日对你单位信息安全等级保护工作进行了监督检查，发现存在下列违规行为（□1 有关信息系统安全保护状况不符合国家信息安全等级保护管理规范和技术标准的要求；□2 未按照《信息安全等级保护管理办法》开展有关工作；□3 不符合其他有关信息安全规定的行为）

1．（具体的不符合行为描述，可自行添加）；

2．；

根据_____，请你单位于_____年__月__日前改正，并在期限届满前将整改情况函告我单位。

在期限届满之前，你单位应当采取必要的安全保护管理和技术措施，确保信息系统安全。

（公安机关印章）

被检查单位： 年 月 日

年 月 日

一式两份，一份交被检查单位，一份附卷。

APPENDIX

E

附录 E　公安机关信息安全等级保护检查工作规范（试行）

中 华 人 民 共 和 国 公 安 部

关于印发《公安机关信息安全等级保护检查工作规范》的通知

公信安[2008]736 号

各省、自治区、直辖市公安厅（局）公共信息网络安全监察总队（处），新疆生产建设兵团公安局公共信息网络安全监察处：

为配合《信息安全等级保护管理办法》（公通字[2007]43 号）的贯彻实施，严格规范公安机关信息安全等级保护检查工作，实现检查工作的规范化、制度化，我局制定了《公安机关信息安全等级保护检查工作规范（试行）》，现印发给你们，请认真贯彻执行。

二〇〇八年六月十日

《公安机关信息安全等级保护检查工作规范（试行）》

第一条 为规范公安机关公共信息网络安全监察部门开展信息安全等级保护检查工作，根据《信息安全等级保护管理办法》（以下简称《管理办法》），制定本规范。

第二条 公安机关信息安全等级保护检查工作是指公安机关依据有关规定，会同主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，督促、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员。

第三条 信息安全等级保护检查工作由市（地）级以上公安机关公共信息网络安全监察部门负责实施。每年对第三级信息系统的运营使用单位信息安全等级保护工作检查一次，每半年对第四级信息系统的运营使用单位信息安全等级保护工作检查一次。

第四条 公安机关开展检查工作，应当按照“严格依法，热情服务”的原则，遵守检查纪律，规范检查程序，主动、热情地为运营使用单位提供服务和指导。

第五条 信息安全等级保护检查工作采取询问情况，查阅、核对材料，调看记录、资料，现场查验等方式进行。

第六条 检查的主要内容：

（一）等级保护工作组织开展、实施情况。安全责任落实情况，信息系统安全岗位和安全管理人员设置情况；

（二）按照信息安全法律法规、标准规范的要求制定具体实施方案和落实情况；

（三）信息系统定级备案情况，信息系统变化及定级备案变动情况；

（四）信息安全设施建设情况和信息安全整改情况；

（五）信息安全管理制度建设和落实情况；

（六）信息安全保护技术措施建设和落实情况；

（七）选择使用信息安全产品情况；

（八）聘请测评机构按规范要求开展技术测评工作情况，根据测评结果开展整改情况；

（九）自行定期开展自查情况；

（十）开展信息安全知识和技能培训情况。

第七条 检查项目：

（一）等级保护工作部署和组织实施情况

（1）下发开展信息安全等级保护工作的文件，出台有关工作意见或方案，组织开展信息安全等级保护工作情况。

（2）建立或明确安全管理机构，落实信息安全责任，落实安全管理岗位和人员。

（3）依据国家信息安全法律法规、标准规范等要求制定具体信息安全工作规划或实施方案。

（4）制定本行业、本部门信息安全等级保护行业标准规范并组织实施。

（二）信息系统安全等级保护定级备案情况

（1）了解未定级、备案信息系统情况以及第一级信息系统有关情况，对定级不准的提出调整建议。

（2）现场查看备案的信息系统，核对备案材料，备案单位提交的备案材料与实际情况相符合情况。

（3）补充提交《信息系统安全等级保护备案表》表四中有关备案材料。

（4）信息系统所承载的业务、服务范围、安全需求等发生变化情况，以及信息系统安全保护等级变更情况。

（5）新建信息系统在规划、设计阶段确定安全保护等级并备案情况。

（三）信息安全设施建设情况和信息安全整改情况

（1）部署和组织开展信息安全建设整改工作。

（2）制定信息安全建设规划、信息系统安全建设整改方案。

（3）按照国家标准或行业标准建设安全设施，落实安全措施。

（四）信息安全管理制度建立和落实情况

（1）建立基本安全管理制度，包括机房安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、备份与恢复、密码管理等制度。

（2）建立安全责任制，系统管理员、网络管理员、安全管理员、安全审计员是否与本单位签订信息安全责任书。

（3）建立安全审计管理制度、岗位和人员管理制度。

（4）建立技术测评管理制度，信息安全产品采购、使用管理制度。

（5）建立安全事件报告和处置管理制度，制定信息系统安全应急处置预案，定期组织开展应急处置演练。

（6）建立教育培训制度，定期开展信息安全知识和技能培训。

（五）信息安全产品选择和使用情况

（1）按照《管理办法》要求的条件选择使用信息安全产品。

（2）要求产品研制、生产单位提供相关材料。包括营业执照，产品的版权或专利证书，提供的声明、证明材料，计算机信息系统安全专用产品销售许可证等。

（3）采用国外信息安全产品的，经主管部门批准，并请有关单位对产品进行专门技术检测。

（六）聘请测评机构开展技术测评工作情况

（1）按照《管理办法》的要求部署开展技术测评工作。对第三级信息系统每年开展一次技术测评，对第四级信息系统每半年开展一次技术测评。

（2）按照《管理办法》规定的条件选择技术测评机构。

（3）要求技术测评机构提供相关材料。包括营业执照、声明、证明及资质材料等。

（4）与测评机构签订保密协议。

（5）要求测评机构制定技术检测方案。

（6）对技术检测过程进行监督，采取了哪些监督措施。

（7）出具技术检测报告，检测报告是否规范、完整，检查结果是否客观、公正。

（8）根据技术检测结果，对不符合安全标准要求的，进一步进行安全整改。

（七）定期自查情况

（1）定期对信息系统安全状况、安全保护制度及安全技术措施的落实情况进行自查。第三级信息系统是否每年进行一次自查，第四级信息系统是否每半年进行一次自查。

（2）经自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位进一步进行安全建设整改。

第八条 各级公安机关按照“谁受理备案，谁负责检查”的原则开展检查工作。具体要求是：

对跨省或者全国联网运行、跨市或者全省联网运行等跨地域的信息系统，由部、省、市级公安机关分别对所受理备案的信息系统进行检查。

对辖区内独自运行的信息系统，由受理备案的公安机关独自进行检查。

第九条 对跨省或者全国联网运行的信息系统进行检查时，需要会同其主管部

门。因故无法会同的，公安机关可以自行开展检查。

第十条 公安机关开展检查前，应当提前通知被检查单位，并发送《信息安全等级保护监督检查通知书》（见附件1）。

第十一条 检查时，检查民警不得少于两人，并应当向被检查单位负责人或其他有关人员出示工作证件。

第十二条 检查中应当填写《信息系统安全等级保护监督检查记录》（以下简称《监督检查记录》，见附件2）。检查完毕后，《监督检查记录》应当交被检查单位主管人员阅后签字；对记录有异议或者拒绝签名的，监督、检查人员应当注明情况。《监督检查记录》应当存档备查。

第十三条 检查时，发现不符合信息安全等级保护有关管理规范和技术标准要求，具有下列情形之一的，应当通知其运营使用单位限期整改，并发送《信息系统安全等级保护限期整改通知书》（以下简称《整改通知》，见附件3）。逾期不改正的，给予警告，并向其上级主管部门通报（《信息安全等级保护检查情况通报书》见附件4）：

（一）未按照《管理办法》开展信息系统定级工作的；

（二）信息系统安全保护等级定级不准确的；

（三）未按《管理办法》规定备案的；

（四）备案材料与备案单位、备案系统不符合的；

（五）未按要求及时提交《信息系统安全等级保护备案登记表》表四的有关内容的；

（六）系统发生变化，安全保护等级未及时进行调整并重新备案的；

（七）未按《管理办法》规定落实安全管理制度、技术措施的；

（八）未按《管理办法》规定开展安全建设整改和安全技术测评的；

（九）未按《管理办法》规定选择使用信息安全产品和测评机构的；

（十）未定期开展自查的；

（十一）违反《管理办法》其他规定的。

第十四条 检查发现需要限期整改的，应当出具《整改通知》，自检查完毕之日起 10 个工作日内送达被检查单位。

第十五条 信息系统运营使用单位整改完成后，应当将整改情况报公安机关，公安机关应当对整改情况进行检查。

第十六条 公安机关实施信息安全等级保护监督检查的法律文书和记录，应当统一存档备查。

第十七条 受理备案的公安机关应该配备必要的警力，专门负责信息安全等级保护监督、检查和指导。从事检查工作的民警应当经过省级以上公安机关组织的信息安全等级保护监督检查岗位培训。

第十八条 公安机关对检查工作中涉及的国家秘密、工作秘密、商业秘密和个人隐私等应当予以保密。

第十九条 公安机关进行安全检查时不得收取任何费用。

第二十条 本规范所称“以上”包含本数（级）。

第二十一条 本规范自发布之日起实施。

附件 1：

（此处印制公安机关名称）

信息安全等级保护监督检查通知书

×公信安 检字[ ] 号

被检查单位名称_____

检查时间_____

检查地点 _____

检查单位 _____

承 办 人_____

批 准 人_____

检查人员_____

填发日期_____

存根

（此处印制公安机关名称）

信息安全等级保护监督检查通知书

×公信安 检字[ ] 号

_____：

根据《中华人民共和国计算机信息系统安全保护条例》和《信息安全等级保护管理办法》规定，我单位决定于____年__月__日至___年__月__日对你单位信息安全等级保护工作落实情况进行监督检查。具体包括下列事项：

□ 1．等级保护工作组织开展、实施情况，安全责任落实情况，信息系统安全岗位和安全管理人员设置情况；

□ 2．按照信息安全法律法规、标准规范制定实施方案和落实情况；

□ 3．信息系统定级备案情况，信息系统变化及定级备案变动情况；

□ 4．信息安全设施建设情况和信息安全整改情况；

□ 5．信息安全管理制度建设和落实情况；

□ 6．信息安全保护技术措施建设和落实情况；

□ 7．选择使用信息安全产品情况；

□ 8．聘请测评机构按规范要求开展技术测评工作情况，根据测评结果开展整改情况；

□ 9．自行定期开展自查情况；

□ 10．开展信息安全知识和技能培训情况。

请你单位有关人员届时参加并做好准备工作。

联系人： 联系电话：

（公安机关印章）

年 月 日

一式两份，一份交被通知单位，一份附卷。

附件 2：

(此处印制公安机关名称)

信息安全等级保护监督检查记录

×公信安 检字[ ] 号

检查民警（签名）_____

被检查单位（部门）名称_____

_____

检查时间_____年 月 日_____

检查地点_____

被检查单位信息安全负责人_____

联系电话 _____

被检查单位信息安全联系人_____

联系电话 _____

记录人（签名）: _____

被检查单位人员（签名）_____

此记录由公安机关存档。

信息安全等级保护监督检查记录单

检查内容	检查结果 （如否说明情况）
一、等级保护工作部署和组织实施情况	
1-1 是否下发开展信息安全等级保护工作的文件，出台有关工作意见或方案，了解组织开展信息安全等级保护工作情况	□是 □否
1-2 是否建立或明确安全管理机构，落实信息安全责任，落实安全管理岗位和人员	□是 □否
1-3 是否依据国家信息安全法律法规、标准规范等要求制定具体信息安全工作规划或实施方案	□是 □否
1-4 是否制定本行业、本部门信息安全等级保护行业标准规范并组织实施	□是 □否
二、信息系统安全等级保护定级备案情况	
2-1 是否有未定级、备案信息系统（如有了解其情况），第一级信息系统定级是否准确	□是 □否
2-2 现场查看备案的信息系统，核对备案材料。备案单位提交的备案材料与实际情况是否相符合	□是 □否
2-3 是否补充提交《信息系统安全等级保护备案表》表四中有关备案材料	□是 □否
2-4 信息系统所承载的业务、服务范围、安全需求等是否发生变化，信息系统安全保护等级是否变更	□是 □否
2-5 新建信息系统是否在规划、设计阶段确定安全保护等级并备案	□是 □否
三、信息安全设施建设情况和信息安全整改情况	
3-1 是否部署和组织开展信息安全建设整改工作	□是 □否
3-2 是否制定信息安全建设规划、信息系统安全整改方案	□是 □否
3-3 是否按照国家标准或行业标准建设安全设施，落实安全措施	□是 □否
四、信息安全管理制度建立和落实情况	
4-1 是否建立基本安全管理制度，包括机房安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、备份与恢复、密码管理等制度	□是 □否
4-2 是否建立安全责任制，系统管理员、网络管理员、安全管理员、安全审计员是否与本单位签订信息安全责任书	□是 □否
4-3 是否建立安全审计管理制度、岗位和人员管理制度	□是 □否
4-4 是否建立技术测评管理制度，信息安全产品采购、使用管理制度	□是 □否
4-5 是否建立安全事件报告和处置管理制度，制定信息系统安全应急处置预案，定期组织开展应急处置演练	□是 □否
4-6 是否建立教育培训制度，是否定期开展信息安全知识和技能培训	□是 □否

续表

检查内容	检查结果（如否说明情况）
五、信息安全产品选择和使用情况	
5-1 是否按照《管理办法》要求的条件选择使用信息安全产品	□是 □否
5-2 是否要求产品研制、生产单位提供相关材料。包括营业执照，产品的版权或专利证书，提供的声明、证明材料，计算机信息系统安全专用产品销售许可证等	□是 □否
5-3 采用国外信息安全产品的，是否经主管部门批准，并请有关单位对产品进行专门技术检测	□是 □否
六、聘请测评机构开展技术测评工作情况	
6-1 是否按照《管理办法》的要求部署开展技术测评工作。对第三级信息系统每年开展一次技术测评，对第四级信息系统每半年开展一次技术测评	□是 □否
6-2 是否按照《管理办法》规定的条件选择技术测评机构	□是 □否
6-3 是否要求技术测评机构提供相关材料。包括营业执照、声明、证明及资质材料等	□是 □否
6-4 是否与测评机构签订保密协议	□是 □否
6-5 是否要求测评机构制定技术检测方案	□是 □否
6-6 是否对技术检测过程进行监督，采取了哪些监督措施	□是 □否
6-7 是否出具技术检测报告，检测报告是否规范、完整，检查结果是否客观、公正	□是 □否
6-8 是否根据技术检测结果，对不符合安全标准要求的，进一步进行安全整改	□是 □否
七、定期自查情况	
7-1 是否定期对信息系统安全状况、安全保护制度及安全技术措施的落实情况进行自查。第三级信息系统是否每年进行一次自查，第四级信息系统是否每半年进行一次自查	□是 □否
7-2 经自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位是否进一步进行安全建设整改	□是 □否
情况说明	

此记录由公安机关存档。

（公安机关印章）

年 月 日

被检查单位主管人员（签名）_____

附件 3：

（此处印制公安机关名称）

信息系统安全等级保护限期整改通知书

×公信安 限字[　　]第　　号

_____：

根据《中华人民共和国计算机信息系统安全保护条例》和《信息安全等级保护管理办法》，我单位工作人员_____于_____年___月___日对你单位信息安全等级保护工作进行了监督检查，发现存在下列违规行为（□ 1 有关信息系统安全保护状况不符合国家信息安全等级保护管理规范和技术标准的要求；□ 2 未按照《信息安全等级保护管理办法》开展有关工作；□ 3 不符合其他有关信息安全规定的行为）

1．（具体的不符合行为描述，可自行添加）；

2．；

根据_____，请你单位于_____年月__日前改正，并在期限届满前将整改情况函告我单位。

在期限届满之前，你单位应当采取必要的安全保护管理和技术措施，确保信息系统安全。

（公安机关印章）

被检查单位：　　年　月　日

一式两份，一份交被检查单位，一份附卷。

附件 4：

（此处印制公安机关名称）

信息安全等级保护检查情况通报书

×公信安 通字[　　] 第　　号

被通报单位名称＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

通报事由＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

办理单位＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

承 办 人＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

批 准 人＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

填发日期＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

存根

（此处印制公安机关名称）

信息安全等级保护检查情况通报书

×公信安 通字[　] 第　号

_____：

根据《中华人民共和国计算机信息系统安全保护条例》和《信息安全等级保护管理办法》，我单位工作人员_____

_____于____年___月___日对_____单位信息安全等级保护工作进行了监督检查，发现存在违规行为并发出《信息系统安全等级保护限期整改通知书》（×公信安 限字[　]第　号）。但在整改期限结束后，未收到整改结果报告，我单位于_____年____月____日对其做出了警告处罚。

鉴于你单位为其上级主管部门，建议你单位督促其按照《信息系统安全等级保护限期整改通知书》的要求开展整改工作，并及时反馈结果。

特此通报。

（公安机关印章）

年　月　日

一式两份，一份交被检查单位，一份附卷。

APPENDIX

F

附录 F　关于加强国家电子政务工程建设项目信息安全风险评估工作的通知

国家发展和改革委员会
中华人民共和国公安部　文件
国　家　保　密　局

发改高技[2008]2071 号

关于加强国家电子政务工程建设项目
信息安全风险评估工作的通知

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委、公安厅、保密局：

为了贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号），加强基础信息网络和重要信息系统安全保障，按照《国家电子政务工程建设项目管理暂行办法》（国家发展和改革委员会令[2007]第 55 号）的有关规定，加

强和规范国家电子政务工程建设项目信息安全风险评估工作，现就有关事项通知如下。

一、国家的电子政务网络、重点业务信息系统、基础信息库以及相关支撑体系等国家电子政务工程建设项目（以下简称电子政务项目），应开展信息安全风险评估工作。

二、电子政务项目信息安全风险评估的主要内容包括：分析信息系统资产的重要程度，评估信息系统面临的安全威胁、存在的脆弱性、已有的安全措施和残余风险的影响等。

三、电子政务项目信息安全风险评估工作按照涉及国家秘密的信息系统（以下简称涉密信息系统）和非涉密信息系统两部分组织开展。

四、涉密信息系统的信息安全风险评估应按照《涉及国家秘密的信息系统分级保护管理办法》、《涉及国家秘密的信息系统审批管理规定》、《涉及国家秘密的信息系统分级保护测评指南》等国家有关保密规定和标准，进行系统测评并履行审批手续。

五、非涉密信息系统的信息安全风险评估应按照《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》和《信息安全风险评估规范》等有关要求，可委托同一专业测评机构完成等级测评和风险评估工作，并形成等级测评报告和风险评估报告。等级测评报告参照公安部门制订的格式编制，风险评估报告参考《国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式》（见附件）编制。

六、电子政务项目涉密信息系统的信息安全风险评估，由国家保密局涉密信息系统安全保密测评中心承担。非涉密信息系统的信息安全风险评估，由国家信息技术安全研究中心、中国信息安全测评中心、公安部信息安全等级保护评估中心等三家专业测评机构承担。

七、项目建设单位应在项目建设任务完成后试运行期间，组织开展该项目的信息安全风险评估工作，并形成相关文档，该文档应作为项目验收的重要内容。

八、项目建设单位向审批部门提出项目竣工验收申请时，应提交该项目信息安

全风险评估相关文档。主要包括：《涉及国家秘密的信息系统使用许可证》和《涉及国家秘密的信息系统检测评估报告》，非涉密信息系统安全保护等级备案证明，以及相应的安全等级测评报告和信息安全风险评估报告等。

九、电子政务项目信息安全风险评估经费计入该项目总投资。

十、电子政务项目投入运行后，项目建设单位应定期开展信息安全风险评估，检验信息系统对安全环境变化的适应性及安全措施的有效性，保障信息系统的安全可靠。

十一、中央和地方共建电子政务项目中的地方建设部分信息安全风险评估工作参照本通知执行。

附件：《国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式》

国家发展改革委　　公　安　部　　国 家 保 密 局

二〇〇八年八月六日

主题词：风险评估　通知

抄送：中央办公厅、全国人民代表大会常务委员会办公厅、国务院办公厅、中国人民政治协商会议全国委员会办公厅、最高法院办公厅、最高检察院办公厅。

附件：

国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式

项 目 名 称：_____

项目建设单位：_____

风险评估单位：_____

年　　月　　日

目　　录

一、风险评估项目概述

1.1 工程项目概况

1.1.1 建设项目基本信息

工程项目名称		
工程项目批复的建设内容	非涉密信息系统部分的建设内容	
	相应的信息安全保护系统建设内容	
项目完成时间		
项目试运行时间		

1.1.2 建设单位基本信息

工程建设牵头部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

工程建设参与部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

如有多个参与部门，分别填写上。

1.1.3 承建单位基本信息

如有多个承建单位，分别填写下表。

企业名称	
企业性质	是国内企业/还是国外企业
法人代表	
通信地址	
联系电话	
电子邮件	

1.2 风险评估实施单位基本情况

评估单位名称	
法人代表	
通信地址	
联系电话	
电子邮件	

二、风险评估活动概述

2.1 风险评估工作组织管理

描述本次风险评估工作的组织体系（含评估人员构成）、工作原则和采取的保密措施。

2.2 风险评估工作过程

工作阶段及具体工作内容。

2.3 依据的技术标准及相关法规文件

2.4 保障与限制条件

需要被评估单位提供的文档、工作条件和配合人员等必要条件，以及可能的限制条件。

三、评估对象

3.1 评估对象构成与定级

3.1.1 网络结构

文字描述网络构成情况、分区情况、主要功能等，提供网络拓扑图。

3.1.2 业务应用

文字描述评估对象所承载的业务及其重要性。

3.1.3 子系统构成及定级

描述各子系统构成。根据安全等级保护定级备案结果，填写各子系统的安全保护等级定级情况表。

各子系统的定级情况表

序　　号	子系统名称	安全保护等级	其中业务信息安全等级	其中系统服务安全等级

3.2 评估对象等级保护措施

按照工程项目安全域划分和保护等级的定级情况，分别描述不同保护等级保护范围内的子系统各自所采取的安全保护措施以及等级保护的测评结果。

根据需要，以下子目录按照子系统重复。

3.2.1 ××子系统的等级保护措施

根据等级测评结果，××子系统的等级保护管理措施情况见附件 1《管理措施表》。

根据等级测评结果，××子系统的等级保护技术措施情况见附件 2《技术指施表》。

3.2.2 子系统 N 的等级保护措施

四、资产识别与分析

4.1 资产类型与赋值

4.1.1 资产类型

按照评估对象的构成，分类描述评估对象的资产构成。详细的资产分类与赋值，以附件形式附在评估报告后面，见附件 3《资产类型与赋值表》。

4.1.2 资产赋值

填写《资产赋值表》。

资产赋值表

序　　号	资产编号	资产名称	子　系　统	资产重要性

4.2　关键资产说明

在分析被评估系统的资产基础上，列出对评估单位十分重要的资产，作为风险评估的重点对象，并以清单形式列出。

关键资产列表

资产编号	子系统名称	应用	资产重要程度权重	其他说明

五、威胁识别与分析

对威胁来源（内部/外部；主观/不可抗力等）、威胁方式、发生的可能性，威胁主体的能力水平等进行列表分析。

5.1　威胁数据采集

5.2 威胁描述与分析

依据《威胁赋值表》（见附件 4），对资产进行威胁源和威胁行为分析。

5.2.1 威胁源分析

填写《威胁源分析表》。

5.2.2 威胁行为分析

填写《威胁行为分析表》。

5.2.3 威胁能量分析

5.3 威胁赋值

填写《威胁赋值表》。

六、脆弱性识别与分析

按照检测对象、检测结果、脆弱性分析分别描述以下各方面的脆弱性检测结果和结果分析。

6.1 常规脆弱性描述

6.1.1 管理脆弱性

6.1.2 网络脆弱性

6.1.3 系统脆弱性

6.1.4 应用脆弱性

6.1.5 数据处理和存储脆弱性

6.1.6 运行维护脆弱性

6.1.7 灾备与应急响应脆弱性

6.1.8 物理脆弱性

6.2 脆弱性专项检测

6.2.1 木马病毒专项检查

6.2.2 渗透与攻击性专项测试

6.2.3 关键设备安全性专项测试

6.2.4 设备采购和维保服务专项检测

6.2.5 其他专项检测

包括：电磁辐射、卫星通信、光缆通信等。

6.2.6 安全保护效果综合验证

6.3 脆弱性综合列表

填写《脆弱性分析赋值表》，见附件 5。

七、风险分析

7.1 关键资产的风险计算结果

填写《风险列表》。

风险列表

资产编号	资产风险值	资产名称

7.2 关键资产的风险等级

7.2.1 风险等级列表

填写《资产风险等级表》。

资产风险等级表

资产编号	资产风险值	资产名称	资产风险等级

7.2.2 风险等级统计

资产风险等级统计表

风险等级	资产数量	所占比例

7.2.3 基于脆弱性的风险排名

基于脆弱性的风险排名表

脆 弱 性	风 险 值	所占比例

7.2.4 风险结果分析

八、综合分析与评价

九、整改意见

附件 1：

管理措施表

序　号	层面/方面	安全控制/措施	落　实	部分落实	没有落实	不适用
	安全管理制度	管理制度				
		制定和发布				
		评审和修订				
	安全管理机构	岗位设置				
		人员配备				
		授权和审批				
		沟通和合作				
		审核和检查				
	人员安全管理	人员录用				
		人员离岗				
		人员考核				
		安全意识教育和培训				
		外部人员访问管理				
	系统建设管理	系统定级				
		安全方案设计				
		产品采购				
		自行软件开发				
		外包软件开发				
		工程实施				
		测试验收				
		系统交付				
		系统备案				
		安全服务商选择				
	系统运维管理	环境管理				
		资产管理				
		介质管理				
		设备管理				
		监控管理和安全管理中心				
		网络安全管理				

续表

序　号	层面/方面	安全控制/措施	落　实	部分落实	没有落实	不适用
		系统安全管理				
		恶意代码防范管理				
		密码管理				
		变更管理				
		备份与恢复管理				
		安全事件处置				
		应急预案管理				
小计						

附件 2：

技术措施表

序　号	层面/方面	安全控制/措施	落实	部分落实	没有落实	不适用
1		物理位置的选择				
		物理访问控制				
		防盗窃和防破坏				
		防雷击				
		防火				
	物理安全	防水和防潮				
		防静电				
		温湿度控制				
		电力供应				
		电磁防护				
		网络结构安全				
		网络访问控制				
		网络安全审计				
	网络安全	边界完整性检查				
		网络入侵防范				
		恶意代码防范				
		网络设备防护				
	主机安全	身份鉴别				

续表

序　号	层面/方面	安全控制/措施	落实	部分落实	没有落实	不适用
		访问控制				
		安全审计				
		剩余信息保护				
		入侵防范				
		恶意代码防范				
		资源控制				
		身份鉴别				
		访问控制				
		安全审计				
		剩余信息保护				
	应用安全	通信完整性				
		通信保密性				
		抗抵赖				
		软件容错				
		资源控制				
	数据安全及备份与恢复	数据完整性				
		数据保密性				
		备份和恢复				

附件 3：

资产类型与赋值表

针对每一个系统或子系统，单独建表。

类　别	项　目	子　项	资产编号	资产名称	资产权重	赋值说明

附件 4：

威胁赋值表

资产名称	编号	威胁																		总分值	威胁等级
		操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	越权使用		

附件 5：

脆弱性分析赋值表

编号	检测项	检测子项	脆弱性	作用对象	赋值	潜在影响	整改建议	标识
1	管理脆弱性检测	机构、制度、人员						V1
		安全策略						V2
		检测与响应脆弱性						V3
		日常维护						V4
		…						V5
2	网络脆弱性检测	网络拓扑及结构脆弱性						V6
		网络设备脆弱性						V7
		网络安全设备脆弱性						V8
		…						V9
3	系统脆弱性检测	操作系统脆弱性						V10
		数据库脆弱性						V11
		…						V12
4	应用脆弱性检测	网络服务脆弱性						V13
		…						V14
5	数据处理和存储脆弱性	数据处理						V15
		数据存储脆弱性						V16
		…						V17

续表

编号	检测项	检测子项		脆弱性	作用对象	赋值	潜在影响	整改建议	标识
6	运行维护脆弱性	安全事件管理							V18
		…							V19
7	灾备与应急响应脆弱性	数据备份							V20
		应急预案及演练							V21
		…							V22
8	物理脆弱性检测	环境脆弱性							V23
		设备脆弱性							V24
		存储介质脆弱性							V25
		…							V26
		…							V27
9	木马病毒检测	远程控制木马							V28
		恶意插件							V29
		…							V30
10	渗透与攻击性检测	现场渗透测试	办公区						V31
			生产区						V32
			服务区						V33
			跨地区						V34
		远程渗透测试							V35
11	关键设备安全性专项检测	关键设备一							V36
		关键设备二							V37
		…							V38
12	设备采购和维保服务	设备采购环节							V39
		维护环节							V40
		…							V41
13	其他检测	…							V42

APPENDIX

G

附录 G　关于开展信息安全等级保护安全建设整改工作的指导意见

中 华 人 民 共 和 国 公 安 部

关于印送《关于开展信息安全等级保护安全建设整改工作的指导意见》的函

公信安[2009]1429 号

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位：

为进一步贯彻落实国家信息安全等级保护制度，指导各地区、各部门在信息安全等级保护定级工作基础上，深入开展信息安全等级保护安全建设整改工作，我部制定了《关于开展信息安全等级保护安全建设整改工作的指导意见》。现印送给你们，请在实际工作中参照。

二〇〇九年十月二十七日

抄送：中央企业。

各省、自治区、直辖市信息安全等级保护工作协调（领导）小组。

关于开展信息安全等级保护安全建设整改工作的指导意见

为进一步贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》和《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》（以下简称《管理办法》）精神，指导各部门在信息安全等级保护定级工作基础上，开展已定级信息系统（不包括涉及国家秘密信息系统）安全建设整改工作，特提出如下意见。

一、明确工作目标

依据信息安全等级保护有关政策和标准，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求，使信息系统安全管理水平明显提高，安全防范能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展，维护国家安全、社会秩序和公共利益，力争在 2012 年底前完成已定级信息系统安全建设整改工作。

二、细化工作内容

（一）开展信息安全等级保护安全管理制度建设，提高信息系统安全管理水平。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的安全管理制度：一是信息安全责任制，明确信息安全工作的主管领导、责任部门、人员及有关岗位的信息安全责任；二是人员安全管理制度，明确人员录用、离岗、考核、教育培训等管理内容；三是系统建设管理制度，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理内容；四是系统运维管理制度，明确机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容。建立并落实监督检查机制，定期对各项

制度的落实情况进行自查和监督检查。

（二）开展信息安全等级保护安全技术措施建设，提高信息系统安全保护能力。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，建立并完善信息系统综合防护体系，提高信息系统的安全防护能力和水平。

（三）开展信息系统安全等级测评，使信息系统安全保护状况逐步达到等级保护要求。选择由省级（含）以上信息安全等级保护工作协调小组办公室审核并备案的测评机构，对第三级（含）以上信息系统开展等级测评工作。等级测评机构依据《信息系统安全等级保护测评要求》等标准对信息系统进行测评，对照相应等级安全保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，提出改进建议，按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告。经测评未达到安全保护要求的，要根据测评报告中的改进建议，制定整改方案并进一步进行整改。各部门要及时向受理备案的公安机关提交等级测评报告。对于重要部门的第二级信息系统，可以参照上述要求开展等级测评工作。

三、落实工作要求

（一）统一组织，加强领导。要按照“谁主管、谁负责”的原则，切实加强对信息安全等级保护安全建设整改工作的组织领导，完善工作机制。要结合各自实际，统一规划和部署安全建设整改工作，制定安全建设整改工作实施方案。要落实责任部门、责任人员和安全建设整改经费。要利用多种形式，组织开展宣传、培训工作。

（二）循序渐进，分步实施。信息系统主管部门可以结合本行业、本部门信息系

统数量、等级、规模等实际情况，按照自上而下或先重点后一般的顺序开展。重点行业、部门可以根据需要和实际情况，选择有代表性的第二、第三、第四级信息系统先进行安全建设整改和等级测评工作试点、示范，在总结经验的基础上全面推开。

（三）结合实际，制定规范。重点行业信息系统主管部门可以按照《信息系统安全等级保护基本要求》等国家标准，结合行业特点，确定《信息系统安全等级保护基本要求》的具体指标；在不低于等级保护基本要求的情况下，结合系统安全保护的特殊需求，在有关部门指导下制定行业标准规范或细则，指导本行业信息系统安全建设整改工作。

（四）认真总结，按时报送。自 2009 年起，要对定级备案、等级测评、安全建设整改和自查等工作开展情况进行年度总结（见《关于报送 2009 年信息安全等级保护工作总结的函》（公信安[2009]1609 号）），于每年年底前报同级公安机关网安部门，各省（自治区、直辖市）公安机关网安部门报公安部网络安全保卫局。信息系统备案单位每半年要填写《信息安全等级保护安全建设整改工作情况统计表》（见附件），并报受理备案的公安机关。

附件：《信息安全等级保护安全建设整改工作情况统计表》

附件：

信息安全等级保护安全建设整改工作情况统计表

<table>
<tr><td colspan="2">01 单位名称</td><td colspan="6"></td></tr>
<tr><td colspan="2">02 单位地址</td><td colspan="6"></td></tr>
<tr><td colspan="2" rowspan="2">03 单位负责人</td><td>姓　　名</td><td></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td colspan="5"></td></tr>
<tr><td colspan="2" rowspan="2">04 单位联系人</td><td>姓　　名</td><td></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td colspan="3"></td></tr>
<tr><td colspan="2">05 信息系统总数</td><td colspan="2"></td><td colspan="2">06 未定级备案信息系统数量</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">07 已定级备案信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="3"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="3"></td></tr>
<tr><td rowspan="6">08 信息系统安全建设整改工作情况</td><td colspan="5">（1）是否明确主管领导、责任部门和具体负责人员</td><td colspan="2">□是 □ 否</td></tr>
<tr><td colspan="5">（2）是否对信息系统安全建设整改工作进行总体部署</td><td colspan="2">□是 □ 否</td></tr>
<tr><td colspan="5">（3）是否对信息系统进行安全保护现状分析</td><td colspan="2">□是 □ 否</td></tr>
<tr><td colspan="5">（4）是否制定信息系统安全建设整改方案</td><td colspan="2">□是 □ 否</td></tr>
<tr><td colspan="5">（5）是否组织开展信息系统安全建设整改工作</td><td colspan="2">□是 □ 否</td></tr>
<tr><td colspan="5">（6）是否组织开展信息系统安全自查工作</td><td colspan="2">□是 □ 否</td></tr>
<tr><td rowspan="2">09 已开展安全建设整改的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="3"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="3"></td></tr>
<tr><td rowspan="2">10 已开展等级测评的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="3"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="3"></td></tr>
<tr><td rowspan="2">11 信息系统发生安全事件、事故数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="3"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="3"></td></tr>
<tr><td rowspan="2">12 已达到等级保护要求的信息系统数量</td><td>第二级系统</td><td></td><td>第三级系统</td><td colspan="3"></td></tr>
<tr><td>第四级系统</td><td></td><td>合　　计</td><td colspan="3"></td></tr>
</table>

填表人：　　审核人：　　填表时间：　　年　月　日

APPENDIX

H

附录 H　信息系统安全等级测评报告模版（试行）

中 华 人 民 共 和 国 公 安 部

关于印发《信息系统安全等级测评报告模版（试行）》的通知

公信安[2009]1487 号

各省、自治区、直辖市公安厅（局）公共信息网络安全监察总队（处），新疆生产建设兵团公安局公共信息网络安全监察处：

为进一步贯彻落实《信息安全等级保护管理办法》（公通字[2007]43 号）和《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）文件精神，规范等级测评活动并按照统一的格式编制测评报告，我局制定了《信息系统安全等级测评报告模版（试行）》，现印发给你们，请认真贯彻落实。

公安部十一局

二〇〇九年十一月六日

报告编号：（××××××××××××-××-××××-××）

信息系统安全等级测评报告模版（试行）

系统名称：_____

被测单位：_____

测评单位：_____

报告时间：_____年_____月_____日

说明：

一、每个备案信息系统单独出具测评报告。

二、测评报告编号为四组数据，各组含义和编码规则如下。

第一组为信息系统备案表编号，由11位数字组成，可以从公安机关颁发的信息系统备案证明（或备案回执）上获得，即证书编号的前11位（前6位为受理备案公安机关代码，后5位为受理备案的公安机关给出的备案单位的顺序编号）。

第二组为年份，由2位数字组成。例如09代表2009年。

第三组为测评机构代码，由四位数字组成。前两位为省级行政区划数字代码的前两位或行业主管部门编号：00为公安部，11为北京，12为天津，13为河北，14为山西，15为内蒙古，21为辽宁，22为吉林，23为黑龙江，31为上海，32为江苏，33为浙江，34为安徽，35为福建，36为江西，37为山东，41为河南，42为湖北，43为湖南，44为广东，45为广西，46为海南，50为重庆，51为四川，52为贵州，53为云南，54为西藏，61为陕西，62为甘肃，63为青海，64为宁夏，65为新疆，66为新疆兵团。90为国防科工局，91为电监会，92为教育部。后两位为公安机关或行业主管部门推荐的测评机构顺序号。

第四组为本年度信息系统测评次数，由两位构成。例如02表示该信息系统本年度测评2次。

信息系统等级测评基本信息表

信息系统					
系统名称				安全保护等级	
备案证明编号				测评结论	
被测单位					
单位名称					
单位地址				邮政编码	
联系人	姓　名		职务/职称		
	所属部门		办公电话		
	移动电话		电子邮件		
测评单位					
单位名称			单位代码		
通信地址				邮政编码	
联系人	姓　名		职务/职称		
	所属部门		办公电话		
	移动电话		电子邮件		
审核批准	编制人	(签名)	编制日期		
	审核人	(签名)	审核日期		
	批准人	(签名)	批准日期		

注：单位代码由受理测评机构备案的公安机关给出。

声　　明

（声明是测评机构对测评报告的有效性前提、测评结论的适用范围以及使用方式等有关事项的陈述。针对特殊情况下的测评工作，测评机构可在以下建议内容的基础上增加特殊声明。）

本报告是×××信息系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测信息系统当时的安全状态有效。当测评工作完成后，由于信息系统发生变更而涉及的系统构成组件（或子系统）都应重新进行等级测评，本报告不再适用。

本报告中给出的测评结论不能作为对信息系统内部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

目　录

报告摘要

（建议不超过800字）

简要描述被测信息系统的名称、安全等级、承载的业务等基本情况。

简要描述测评范围和主要内容。

简要描述测评指标的符合性情况，给出测评结论（包括符合、基本符合和不符合）。

简要描述测评中发现的主要问题和危害，并提出安全建设整改建议。

第 1 章　测评项目概述

1.1　测评目的

1.2　测评依据

列出开展测评活动所依据的文件、标准和合同等。

1.3　测评过程

描述等级测评工作流程，包括测评工作流程图、各阶段完成的关键任务和工作的时间节点等内容。

1.4　报告分发范围

说明等级测评报告正本的份数与分发范围。

第 2 章　被测信息系统情况

参照备案信息简要描述信息系统。

2.1　承载的业务情况

描述信息系统承载的业务、应用等情况。

2.2　网络结构

给出被测信息系统的拓扑结构示意图，并基于示意图说明被测信息系统的网络

结构基本情况，包括功能/安全区域划分、隔离与防护情况、关键网络和主机设备的部署情况和功能简介、与其他信息系统的互联情况和边界设备以及本地备份和灾备中心的情况。

2.3 系统构成

2.3.1 业务应用软件

以列表的形式给出被测信息系统中的业务应用软件（包括含中间件等应用平台软件），描述项目包括软件名称、主要功能简介。

序　　号	软件名称	主要功能	重要程度①
…	…	…	…

2.3.2 关键数据类别

以列表形式描述具有相近业务属性和安全需求的数据集合。

序　　号	数据类别	所属业务应用	主机/存储设备	重要程度
…	…	…		…

2.3.3 主机/存储设备

以列表形式给出被测信息系统中的主机设备，描述主机设备的项目包括设备名称、操作系统、数据库管理系统以及承载的业务应用软件系统。

① 依据《信息系统安全等级测评过程指南》判定。

序　号	设备名称	操作系统/数据库管理系统	业务应用软件
…	…		…

2.3.4　网络互联设备

以列表形式给出被测信息系统中的网络互联设备。

序　号	设备名称	用　途	重要程度
…	…	…	…

2.3.5　安全设备

以列表形式给出被测信息系统中的安全设备。

序　号	设备名称	用　途	重要程度
…	…	…	…

2.3.6　安全相关人员

以列表形式给出与被测信息系统安全相关的人员情况。相关人员包括（但不限于）安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、机房管理人员、资产管理员、业务操作员、安全审计人员等。

序　号	姓　名	岗位/角色	联系方式
…	…	…	…

2.3.7 安全管理文档

以列表形式给出与信息系统安全相关的文档，包括管理类文档、记录类文档和其他文档。

序　　号	文档名称	主要内容
…	…	…

2.4 安全环境

描述被测信息系统的运行环境中与安全相关的部分，并以列表形式给出被测信息系统的威胁列表并赋值。威胁赋值是基于历史统计或者行业判断进行的，具体内容可参考《风险评估规范》。

序　　号	威胁分(子)类	描述	威胁赋值
…	…	…	…

2.5 前次测评情况

简要描述前次等级测评发现的主要问题和测评结论。

第 3 章　等级测评范围与方法

3.1 测评指标

测评指标包括基本指标和特殊指标两部分。

3.1.1 基本指标

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《基本要求》中对应级别的安全要求作为等级测评的基本指标。

鉴于信息系统的复杂性和特殊性（如某些信息系统未部署数据库服务器），基本指标中可能存在部分不适用项，可以在单元测评时进行识别。

安全分类[①]	安全子类[②]	测评项数	备　注
…	…	…	

3.1.2 特殊指标

结合行业和系统的实际，以列表形式给出《基本要求》未覆盖或者高于《基本要求》的安全要求。

安全分类	安全子类	特殊要求描述	测评项数
…	…		…

3.2 测评对象

3.2.1 测评对象选择方法

描述测评对象的选择规则和方法。

① 安全分类对应基本要求中的物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等 10 个安全要求类别。

② 安全子类是对安全分类的进一步细化，在《基本要求》目录级别中对应安全分类的下一级目录。

3.2.2 测评对象选择结果

1．机房

序　　号	机房名称	物理位置

2．业务应用软件

序　　号	软件名称	主要功能
…	…	…

3．主机（存储）操作系统

序　　号	设备名称	操作系统/数据库管理系统
…	…	…

4．数据库管理系统

序　　号	设备名称	操作系统/数据库管理系统
…	…	…

5．网络互联设备操作系统

序　　号	操作系统名称	设备名称
…	…	…

6．安全设备操作系统

序　号	操作系统名称	设备名称
…	…	…

7．访谈人员

序　号	姓　名	岗位/职责
…	…	…

8．安全管理文档

序　号	文档名称	主要内容
…	…	…

3.3　测评方法

描述等级测评工作中采用的访谈、检查、测试和风险分析等方法。

第 4 章　单元测评

等级测评内容包括“3.1 测评指标”中涉及的物理安全、网络安全、主机安全等10 个安全分类，具体内容由结果记录、问题分析和结果汇总等三部分构成。

4.1　物理安全

4.1.1　结果记录

以表格形式给出物理安全的现场测评结果。

安全子类	测评指标	结果记录	符合情况
物理位置的选择	…	…	…
	…	…	…
物理访问控制	…	…	…
…	…	…	…

4.1.2 结果汇总

针对不同测评指标子类对物理安全的单项测评结果进行汇总和统计。

4.1.3 问题分析

针对物理安全测评结果中存在的部分符合项或不符合项加以汇总和分析，形成安全问题描述。

4.2 网络安全

4.2.1 结果记录

4.2.2 结果汇总

4.2.3 问题分析

4.3 主机安全

4.3.1 结果记录

4.3.2 结果汇总

4.3.3 问题分析

4.4 应用安全

4.4.1 结果记录

4.4.2 结果汇总

4.4.3 问题分析

4.5 数据安全及备份恢复

4.5.1 结果记录

4.5.2 结果汇总

4.5.3 问题分析

4.6 安全管理制度

4.6.1 结果记录

4.6.2 结果汇总

4.6.3 问题分析

4.7 安全管理机构

4.7.1 结果记录

4.7.2 结果汇总

4.7.3 问题分析

4.8 人员安全管理

4.8.1 结果记录

4.8.2 结果汇总

4.8.3 问题分析

4.9 系统建设管理

4.9.1 结果记录

4.9.2 结果汇总

4.9.3 问题分析

4.10 系统运维管理

4.10.1 结果记录

4.10.2 结果汇总

4.10.3 问题分析

第 5 章 整体测评

从安全控制间、层面间、区域间和系统结构等方面对单元测评的结果进行验证、分析和整体评价。具体内容参见《信息安全技术 信息系统安全等级保护测评要求》。

5.1 安全控制间安全测评

5.2 层面间安全测评

5.3 区域间安全测评

5.4 系统结构安全测评

第 6 章 测评结果汇总

一是以表格形式汇总测评结果。表格以不同颜色对测评结果进行区分，部分符合的安全子类采用黄色标识，不符合的安全子类采用红色标识。

序 号	安全分类	安全子类	符合情况		
			符 合	部分符合	不 符 合
1	物理安全	物理位置的选择			
2		物理访问控制			
3		防盗窃和防破坏			

续表

序　号	安全分类	安全子类	符合情况		
			符　合	部分符合	不 符 合
4	物理安全	防雷击			
5		防火			
6		防水和防潮			
7		防静电			
8		温湿度控制			
9		电力供应			
10		电磁防护			
…	…	…	…	…	…
统计			7	2	1

二是以柱状图形式统计不同设备和安全子类的测评结果。

三是以表格形式汇总信息系统中存在的安全问题。

第 7 章　风险分析和评价

依据等级保护的相关规范和标准，采用风险分析的方法分析信息系统等级测评结果中存在的安全问题（等级测评结果中部分符合项或不符合项的汇总结果）可能对信息系统安全造成的影响。

分析过程包括：

（1）判断安全问题被威胁利用的可能性，可能性的取值范围为高、中和低；

（2）判断安全问题被威胁利用后，对信息系统安全（业务信息安全和系统服务安全）造成的影响程度，影响程度取值范围为高、中和低；

（3）综合（1）和（2）的结果对信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低；

（4）结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

以列表形式给出等级测评发现安全问题以及风险分析和评价情况。

系统安全问题风险分析和评价表

序　　号	问题描述	关联资产[①]	关联威胁[②]	风 险 值	风险评价
一					
二					
三					
…					

第 8 章　等级测评结论

综合第 5、第 6、第 7 章的测评与分析结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论，应表述为“符合”、“基本符合”或者“不符合”。

测评结论的判别依据如下：

测评结论	判别依据
符合	等级测评结果中不存在部分符合项或不符合项
基本符合	等级测评结果中存在部分符合项或不符合项，但不会导致信息系统面临高等级安全风险
不符合	等级测评结果中存在部分符合项或不符合项，导致信息系统面临高等级安全风险

第 9 章　安全建设整改建议

针对系统存在的主要安全问题提出安全建设整改建议。

① 如风险值和评价相同，可填写多个关联资产。

② 对于多个关联的情况，应分别填写。

APPENDIX

I

附录Ⅰ　关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知

中 华 人 民 共 和 国 公 安 部

关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知

公信安[2010]303 号

各省、自治区、直辖市公安厅、局网络安全保卫（公共信息网络安全监察、网络警察）总队（处）、新疆生产建设兵团公安局公共信息网络安全监察处：

为进一步贯彻落实公安部《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）精神，加快信息安全等级保护测评体系建设，提高测评机构能力，规范测评活动，确保信息安全等级保护安全建设整改工作顺利进行，满足信息安全等级保护工作的迫切需要，决定在全国部署开展信息安全等级保护测评体系建设和等级测评工作。现将有关事项通知如下。

一、工作目标

（一）通过广泛宣传和正确引导，鼓励更多的有关企事业单位从事信息安全等级测评工作，满足信息安全等级保护测评工作的迫切需要。

（二）通过对测评机构进行统一的能力评估和严格审查，保证测评机构的水平和能力达到有关标准规范要求。

（三）加强对测评机构的安全监督，规范其测评活动，保证为备案单位提供客观、公正和安全的测评服务。

（四）督促备案单位开展等级测评工作，为开展等级保护安全建设整改工作奠定基础，使信息系统安全保护状况逐步达到等级保护要求。

二、工作内容

各地要按照《关于开展信息安全等级保护安全建设整改工作的指导意见》要求，结合本地实际组织开展以下工作。

（一）统筹规划，正确引导，积极稳妥地推动等级测评机构建设。结合本地已定级备案信息系统数量和分布情况，从满足等级测评工作的实际需要出发，统筹规划、合理布局测评机构的规模和数量，积极引导本地符合规定条件、有良好信誉的企事业单位从事等级测评工作，按照成熟一个发展一个的原则，有计划、积极稳妥地推动测评机构建设。

（二）规范流程，严格把关，确保测评机构的水平和能力符合测评工作要求。依据《信息安全等级保护测评工作管理规范》，对申请成为测评机构的单位严格把关，按照申请受理、测评能力评估、审核、推荐的流程，认真开展测评机构评审和推荐工作。同时，要加强对等级测评机构的监督管理和指导，确保测评机构的水平和能力符合要求以及测评活动客观、公正和安全。

（三）督促备案单位开展信息系统等级测评工作，确保安全建设整改工作的顺利开展。督促信息系统备案单位尽快委托测评机构开展等级测评，2010 年底前完成测

评体系建设，并完成 30%第三级（含）以上信息系统的测评工作，2011 年底前完成第三级（含）以上信息系统的测评工作，2012 年底之前完成第三级（含）以上信息系统的安全建设整改工作。

三、工作要求

（一）高度重视，落实责任。要充分认识开展等级测评体系建设和等级测评工作的重要性，加强组织领导，落实责任。确定主管领导，落实专门管理人员，负责受理申请、审核、监督管理以及其他日常对测评机构、测评人员的管理工作。

（二）制定计划，加强监督。要尽快确定本地等级测评体系建设和测评工作的计划，制定贯彻实施意见和方案。要督促、检查本地测评机构依据有关标准开展等级测评活动，按照《信息系统安全等级测评报告模版（试行）》（公信安[2009]1487号）编制测评报告。

（三）加强指导，积极宣传。要加强对本地备案单位和测评机构等级测评工作的指导，指导测评机构对测评人员开展教育培训，不断提高测评人员的安全意识和业务能力。要充分利用会议、网站和其他媒体，加大对等级测评工作有关政策和相关标准的宣传力度，推动等级测评工作的顺利开展。

各地开展等级保护测评体系建设和测评工作的情况要及时上报。工作中有何问题，请及时报我局。

附件：《信息安全等级保护测评工作管理规范》（试行）

APPENDIX

J

附录 J　信息安全等级保护测评工作管理规范（试行）

第一条 为加强信息安全等级保护测评机构建设和管理，规范等级测评活动，保障信息安全等级保护测评工作（以下简称“等级测评工作”）的顺利开展，根据《信息安全等级保护管理办法》等有关规定，制订本规范。

第二条 本规范适用于等级测评机构和人员及其测评活动的管理。

第三条 等级测评工作，是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动。

等级测评机构，是指具备本规范的基本条件，经能力评估和审核，由省级以上信息安全等级保护工作协调（领导）小组办公室（以下简称为“等保办”）推荐，从事等级测评工作的机构。

第四条 省级以上等保办负责等级测评机构的审核和推荐工作。

公安部信息安全等级保护评估中心（以下简称“评估中心”）负责测评机构的能力评估和培训工作。

第五条 等级测评机构应当具备以下基本条件：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）产权关系明晰，注册资金 100 万元以上；

（四）从事信息系统检测评估相关工作两年以上，无违法记录；

（五）工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录；

（六）具有满足等级测评工作的专业技术人员和管理人员，测评技术人员不少于 10 人；

（七）具备必要的办公环境、设备、设施，使用的技术装备、设施应当符合《信息安全等级保护管理办法》对信息安全产品的要求；

（八）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

（九）对国家安全、社会秩序、公共利益不构成威胁；

（十）应当具备的其他条件。

第六条 测评机构及其测评人员应当严格执行有关管理规范和技术标准，开展客观、公正、安全的测评服务。

测评机构可以从事等级测评活动以及信息系统安全等级保护定级、安全建设整改、信息安全等级保护宣传教育等工作的技术支持。不得从事下列活动：

（一）影响被测评信息系统正常运行，危害被测评信息系统安全；

（二）泄露知悉的被测评单位及被测信息系统的国家秘密和工作秘密；

（三）故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具等级测评报告；

（四）未按规定格式出具等级测评报告；

（五）非授权占有、使用等级测评相关资料及数据文件；

（六）分包或转包等级测评项目；

（七）信息安全产品开发、销售和信息系统安全集成；

（八）限定被测评单位购买、使用其指定的信息安全产品；

（九）其他危害国家安全、社会秩序、公共利益以及被测单位利益的活动。

第七条 申请成为等级测评机构的单位（以下简称“申请单位”）应当向省级以上等保办申请。

国家信息安全等级保护工作协调小组办公室负责受理隶属国家信息安全职能部门和重点行业主管部门申请单位提出的申请。省级等保办负责受理本省（区、直辖市）申请单位提出的申请。

申请单位申请时，等保办应当告知测评机构的条件、从事的业务范围以及禁止行为等内容，使申请单位清楚了解测评机构的权利和义务。

第八条 知悉有关规定并愿意成为测评机构的申请单位，可以向省级以上等保办提出书面申请，如实填写《信息安全等级保护测评机构申请表》（见附件 1）。

申请单位的人员应当如实填写人员基本情况表，并承诺对信息的真实性和有效性负责。

省级以上等保办对申请单位进行初审，初审通过的，应当告知申请单位到评估中心进行测评能力评估。

第九条 评估中心按照有关标准规范，在 30 个工作日内完成对申请单位的材料审查和现场核查工作。

测评人员参加由评估中心举办的专门培训、考试并取得评估中心颁发的《等级测评师证书》（等级测评师分为初级、中级和高级）。等级测评人员需持等级测评师证上岗。

评估中心综合评估申请单位的测评能力，对测评能力评估合格的，出具评估报告。

第十条 省级以上等保办组织专家对通过测评能力评估的申请单位及其测评人员进行审核。

第十一条 通过审核的，由省级以上等保办向申请单位颁发信息安全等级保护测评机构推荐证书（见附件 2），并向社会公布测评机构推荐目录。

省级等保办将测评机构推荐目录报国家信息安全等级保护工作协调小组办公室，国家信息安全等级保护工作协调小组办公室汇总公布《全国信息安全等级保护测评机构推荐目录》。

第十二条 测评机构应当按照公安部统一制订的《信息系统安全等级测评报告模版》格式出具测评报告，根据信息系统规模和所投入的成本，合理收取测评服务费用。

第十三条 省级以上等保办每年对所推荐的测评机构进行检查，测评机构应提交《信息安全等级保护测评机构检查表》（见附件 3）。

第十四条 测评机构名称、法人等事项发生变化的，或者其等级测评师变动的，测评机构应在三十日内向受理申请的省级以上等保办办理变更手续。

第十五条 测评机构应当严格遵循申诉、投诉及争议处理制度，妥善处理争议事件，及时采取纠正和改进措施。

第十六条 测评机构或者其测评人员违反本规范第六条规定之一或年度检查未通过的，由省级以上等保办责令其限期改正；逾期不改正的，给予警告，直至取消测评机构的推荐证书或等级测评师证书，并向社会公告；造成严重损害的，由相关部门依照有关法律、法规予以处理。

第十七条 测评机构或者测评人员违反本规范的规定，给被测评单位造成损失的，应当依法承担民事责任。

第十八条 本规范由国家信息安全等级保护工作协调小组办公室负责解释。

第十九条 本规范中省级以上含省级。

第二十条 本规范自发布之日起施行。

附件 1：《信息安全等级保护测评机构申请表》

附件 2：信息安全等级保护测评机构推荐证书样式

附件 3：《信息安全等级保护测评机构检查表》

附件 1：

编号：（×）×××　　年　月　日

信息安全等级保护测评机构
申 请 表

单位名称： _____

单位地址： _____

申请日期： _____

国家信息安全等级保护工作协调小组办公室制

填表说明：（封皮背面）

1．申请表编号说明：（×）×××　　年　月　日，×是各地行政区划简称，×××是申请书编号。

2．申请表各项内容应如实填写，文字表述明确。

3．申请表签字盖章方为有效。应由申请单位法定代表人签字；委托代表人签字的，应出具有效的委托书。

4．申请表中“单位类型”应按照单位营业执照填写。

5．如所填内容超出表格时，可添加附页。

6．申请单位人员基本情况表每人填写一份。

7．申请表一式两份。

申请单位基本情况表

<table>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="5"></td></tr>
<tr><td rowspan="2">法定代表人</td><td colspan="2" rowspan="2"></td><td>手　机</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td></tr>
<tr><td rowspan="2">单位负责人</td><td colspan="2" rowspan="2"></td><td>手　机</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td></tr>
<tr><td rowspan="3">单位联系人</td><td colspan="2" rowspan="3"></td><td>手　机</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>电子邮箱</td><td colspan="2"></td></tr>
<tr><td>注册资本</td><td colspan="2"></td><td>单位类型</td><td colspan="2"></td></tr>
<tr><td>员工总数</td><td></td><td>管理人员数</td><td></td><td>技术人员数</td><td></td></tr>
<tr><td>测评机构应当具备的基本条件</td><td colspan="5">（请在符合的条件序号前□内打“√”）
□ 1. 在中国境内注册成立（港澳台地区除外）；
□ 2. 由中国公民投资、中国法人投资或国家投资的企事业单位（港澳台地区除外）；
□ 3. 产权关系明晰，注册资金 100 万元以上；
□ 4. 从事信息系统检测评估相关工作两年以上；
□ 5. 工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录；
□ 6. 具有满足等级测评工作的专业技术人员和管理人员，测评技术人员不少于 10 人；
□ 7. 具备必要的办公环境、设备、设施，使用的技术装备、设施应当符合《信息安全等级保护管理办法》对信息安全产品的要求；
□ 8. 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。
□ 9. 对国家安全、社会秩序、公共利益不构成威胁。</td></tr>
</table>

续表

业务范围及主营业务	（按营业执照填写）
从事信息系统检测评估相关工作情况	（近年来从事信息系统检测评估相关工作的业绩，需要列举已完成项目的范例）

续表

设备设施配备情况	（等级测评所需的测试实验环境、测评工作平台、专门工具、测试与评估设备及其它服务保障设施情况；设备类别清单）
安全保密管理等制度情况	（为加强内部规范管理，适应等级测评业务安全保密要求而采取的人员管理、安全保密管理、设备使用管理、测评质量控制管理等方面的措施和制度建设情况）

续表

测评技术力量情况	（技术人才数量、层次、培训、承担重大课题、项目情况）
申请表附件	（请在提供的材料序号前□内打“√”） □ 1.营业执照复印件 □ 2.法定代表人及股东身份证复印件 □ 3.申请单位人员基本情况表（每人填写一份） □ 4.股权（资本）结构说明 □ 5.申请单位组织结构表 □ 6.相关资质能力证书复印件
申请单位声明	我单位知悉信息安全等级保护测评机构的责任义务，现申请成为信息安全等级保护测评机构，自愿服从并接受相关安全保密、测评规范管理，并保证所提交的有关材料均真实有效。如有虚假，本单位愿承担一切后果及相关法律责任。 其他特别声明事项： 法定代表人：（ 签字 ） 申请单位: （盖章） 年 月 日

申请单位人员基本情况表

姓　　名		性　　别		免冠照片
出生年月		国　　籍		
政治面貌		出 生 地		
最高学历		身份证号		
护照号码		绿卡号码		
户籍地址			邮编	
居住地址			邮编	
职　　务			职称	
电子邮箱			电话	
犯罪记录				
业务能力和专长				
直系亲属涉外关系				

教育背景（从大专填写）			
时　间	院 校 名 称	专业方向	见证人
培训经历			
时　间	培训机构名称	培训项目	证书名称
工作经历			
时间	单位名称	职务\职称	见证人

所提供附件	（请在提供的材料序号前□内打“√”） □ 1．身份证复印件 □ 2．最高学历证书复印件 □ 3．相关认证、技能证书复印件
个人郑重声明	**郑重声明** 本人清楚国家对等级测评从业人员的安全审查和等级测评技术能力等方面的要求，愿意服从并遵守有关安全保密等管理规范，并承诺按照相关标准规范要求和规定认真履行工作职责。本人自愿接受关于本人的审查，所提供的全部资料均真实有效，如有虚假，本人将承担由此造成的一切后果及相关法律责任。 个人签名： 单位盖章： 日期：

安 全 保 证 承 诺 书

等级测评工作是等级保护工作的重要组成部分，直接关系信息系统安全，作为从事信息安全等级测评工作的机构，本单位及其人员知悉测评机构的责任义务和工作规范，愿意服从并接受各项安全保密管理，并承诺按照有关标准规范开展等级测评工作，保证测评工作的公平、公正、安全，如有虚假或有违反测评管理规范的行为，本单位将承担由此造成的一切后果及相关的法律责任。

法定代表人签字：

单位盖章：

年　月　日

<table>
<tr><td colspan="3">以下内容由省级以上等保办填写</td></tr>
<tr><td>能力评估情况</td><td colspan="2">（能力评估报告摘录，评估情况及结论。）</td></tr>
<tr><td>等级测评师培训获证情况</td><td colspan="2"></td></tr>
<tr><td>专家审核意见</td><td colspan="2">专家组长：（签字）
年　　月　　日</td></tr>
<tr><td>省级以上等保办推荐意见</td><td>承办人：（签字）
年　　月　　日</td><td>负责人：（签字/盖章）
年　　月　　日</td></tr>
</table>

附件 2：

测评机构推荐证书样式

证书编号：（省简称）－0001

信息安全等级保护测评机构推荐证书

×××测评机构：

经审查，你单位符合信息安全等级保护测评机构有关规范要求，具备从事信息系统等级测评工作能力，现予以推荐。

特发此证。

发证日期：2010-03-06

有效期至：2013-03-06

信息安全等级保护专用章

测评机构推荐证书（副本）样式

证书编号：（省简称）－0001

信息安全等级保护测评机构推荐证书

（副　本）

机构名称：

地　　址：

法定代表人：

发证日期：　　有效期至：

年度检查情况：

第一次检查时间（　年　月　日）	第二次检查时间（　年　月　日）	第三次检查时间（　年　月　日）
检查情况： 负责人：（签字/盖章） 年　月　日	检查情况： 负责人：（签字/盖章） 年　月　日	检查情况： 负责人：（签字/盖章） 年　月　日

附件 3：

编号：（×）×××　年　月　日

信息安全等级保护测评机构
检　查　表

测评机构名称：_____（盖章）

测评机构地址：_____

检 查 日 期：_____

国家信息安全等级保护工作协调小组办公室制

填表说明：（封皮背面）

1．编号（×）×××　年　月　日说明：×是各地行政区划简称，×××是检查表编号。

2．检查表各项内容应如实填写，文字表述明确，不得弄虚作假。

3．检查表盖章方为有效。

4．检查表中“单位类型”应按照单位营业执照填写。

5．如所填内容超出表格时可另添加附页。

6．测评结论按照合格、基本合格、不合格填写。

7．负责人为省级以上等保办领导。

8．检查表一式两份。

<table>
<tr><td>测评机构名称</td><td colspan="7"></td></tr>
<tr><td>测评机构地址</td><td colspan="7"></td></tr>
<tr><td rowspan="2">法定代表人</td><td colspan="2" rowspan="2"></td><td>办公电话</td><td colspan="3"></td></tr>
<tr><td>手　　机</td><td colspan="3"></td></tr>
<tr><td rowspan="2">单位联系人</td><td colspan="2" rowspan="2"></td><td>办公电话</td><td colspan="3"></td></tr>
<tr><td>手　　机</td><td colspan="3"></td></tr>
<tr><td>测评系统总数</td><td></td><td>四级</td><td></td><td>三级</td><td></td><td>二级</td><td></td></tr>
<tr><td>测评项目总值</td><td colspan="7">（万元）</td></tr>
<tr><td>测评工作开展情况</td><td colspan="7"></td></tr>
</table>

测评人员教育培训情况	
质量控制保障措施	
人员变更情况	

信息系统等级测评项目汇总表				
序号	信息系统名称	等级	所属单位	结论

承办人检查意见	（是否有违反管理规范行为，是否同意通过年度检查） 承办人：（签字） 年　　月　　日
负责人意见	 负责人：（签字） 年　　月　　日

APPENDIX

K

附录K　信息安全等级保护安全建设指导委员会专家名单

专家委主任、副主任				
主　任	沈昌祥	男	海军计算技术研究所	院　士
副主任	方滨兴	男	北京邮电大学校长	院　士
专家委成员				
1	崔书昆	男	解放军信息安全测评认证中心	研究员
2	王立福	男	北京大学软件工程国家工程研究中心	教　授
3	袁文恭	男	国家信息安全工程技术研究中心	研究员
4	冯登国	男	信息安全共性技术国家工程研究中心	主任/教授
5	王　娜	女	国家发改委高技术司信息化处	处　长
6	郭全明	男	人民银行科技司安全处	处　长
7	张瑞芝	女	广电总局安调中心	副总工
8	刘祖泷	男	铁道部信息办	处　长
9	李建彬	男	税务总局信息中心	处　长
10	闫宏强	男	工信部通保局	副处长
11	李宏图	男	海关总署	处　长
12	倪吉祥	男	国家电监会信息中心	主任
13	马晓东	男	公安部科信局	总　工
14	王才有	男	卫生部统计信息中心	副主任
15	蔡　阳	男	水利部水利信息中心	主　任
16	王继业	男	国家电网公司信息化工作部	副主任
17	罗　凯	男	证监会信息中心	总　工

续表

18	栗演兵	男	民政部信息中心	副主任
19	顾炳中	男	国土资源部信息中心	总　工
20	周德铭	男	审计署信息化建设办公室	主　任
21	王连印	男	国家质检总局信息中心	副主任
22	刘长虹	男	国资委信息办	副主任
23	朱建平	男	公安部等级保护评估中心	副主任
24	李京春	男	国家信息技术安全研究中心	总　工
25	王　军	男	中国信息安全测评中心	总　工
26	顾　健	男	公安部信息安全产品检测中心	副主任
27	陈建民	男	病毒产品检测中心	副主任
28	刘科全	男	联想网御	总　裁
29	赵显东	男	启明星辰解决方案中心	总　监
30	孙　铁	男	绿盟科技	技术顾问

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
Broadview®
www.broadview.com.cn

《信息安全等级保护政策培训教程》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；
2. 本书作者的见面会信息或网络视频的沟通活动；
3. 相关领域的培训优惠。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下两种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1．短信

您只需编写如下短信：B10885+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）

为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2．电子邮件

您可以发邮件至jsj@phei.com.cn或editor@broadview.com.cn。

如果您选择第2种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

（1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；

（2）您了解新书信息的途径、影响您购买图书的因素；

（3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B10885+退订”至10666666789即可，或者编写邮件“B10885+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

华信知识服务平台是电子工业出版社（PHEI）主办的，基于数据库和互联网的，涵盖按需出版、会议、培训等多项业务的知识服务集团，已经成功举办过多次培训（软件安全编程培训）和会议（中国计算机网络安全应急年会、中国软件安全峰会），我们将邀请**本书作者和相关专家**开展“信息安全等级保护”的相关培训，咨询电话：010-88254012，通过电话登记者将获得**培训优惠。**

通信地址：北京万寿路 173 信箱　博文视点（100036）
电话：010-88254012　　传真：010-88254490
E-mail：panxin@phei.com.cn，editor@broadview.com.cn

反侵权盗版声明

Broadview®
www.broadview.com.cn
博文视点·IT出版旗舰品牌
技术凝聚实力·专业创新出版

信息安全等级保护政策培训教程

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。开展信息安全等级保护工作不仅是保障重要信息系统安全的重大措施，也是一项事关国家安全、社会稳定、国家利益的重要任务。

本书内容包括

◆信息安全等级保护制度的主要内容
◆信息安全等级保护政策体系和标准体系
◆信息系统定级与备案工作
◆信息安全等级保护安全建设整改工作
◆信息安全等级保护等级测评工作
◆安全自查和监督检查

上架建议：计算机>信息安全

ISBN 978-7-121-10885-3

9 787121 108853 >

定价：45.00元

策划编辑：毕　宁
责任编辑：许　艳
责任美编：侯士卿